WORKSHOP

Requested by the SEDE subcommittee

The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict

Authors:
Stéphane DUGUIN, Pavlina PAVLOVA

European Parliament coordinator:
Policy Department for External Relations
Directorate General for External Policies of the Union
PE 702.594 - September 2023

EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

WORKSHOP

The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict

ABSTRACT

On 24 February 2022, the Russian Federation carried out a further military invasion of Ukraine, violating the UN Charter. The ongoing international armed conflict in Ukraine raises concerns about harm and impact caused to the civilian population, and the protection of civilians and civilian infrastructure which are affected by both kinetic and cyberattacks. This report analyses the magnitude of the cyber dimension of the war in Ukraine, its impact, and the lessons learned with the aim to increase understanding about the threat environment, and strengthen cyber resilience and defence capabilities across the EU and in neighbouring countries.

EP/EXPO/A/COMMITTEE/FWC/2019-01/Lot4/1/C/20
September 2023 - PE 702.594

EN

AUTHORS

- Stéphane DUGUIN, CyberPeace Institute, Geneva, Switzerland
- Pavlina PAVLOVA, CyberPeace Institute, Geneva, Switzerland

PROJECT COORDINATOR (CONTRACTOR)

- Joanna SMĘTEK, Ecorys Poland, contractor
- Katarzyna LUBIANIEC, Ecorys Poland, contractor

PEER-REVIEW

- Giorgi IASHVILI, Cyber Trust

This paper was requested by the European Parliament's subcommittee on Security and Defence (SEDE).

The content of this document is the sole responsibility of the authors, and any opinions expressed herein do not necessarily represent the official position of the European Parliament.

CONTACTS IN THE EUROPEAN PARLIAMENT

Coordination: Jérôme LEGRAND, Policy Department for External Relations

Editorial assistant: Grégory DEFOSSEZ, Inge BRYS

Feedback is welcome. Please write to jerome.legrand@europarl.europa.eu

To obtain copies, please send a request to poldep-expo@europarl.europa.eu

VERSION

English-language manuscript completed on 04 September 2023.

This paper will be published on the European Parliament's online database, 'Think Tank'

Table of contents

I. Working paper

BRIEFING

The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict

Table of contents

1 Introduction

1.1 Purpose

On 24 February 2022, the Russian Federation carried out a further military invasion of Ukraine, violating the UN Charter[1]. The ongoing international armed conflict raises concerns about harm and impact caused to the civilian population, and the protection of civilians and civilian infrastructure which are affected by both kinetic and cyberattacks.

The term cyber war – used to refer to a method of warfare whereby state and non-state actors aim to penetrate another computer or network to cause damage or disruption – is being routinely used in this war of aggression. While experts disagree over the precise scale, impact, and importance of Russian cyberattacks and operations in reaching the country's strategic goals, cyberspace is now an established and fast-developing domain of conflict.

As the new European defence doctrine, approved by the European Council in March 2022, the Strategic Compass[2] recognises cyber as a domain of warfare that must be protected through cooperation and close coordination. This is an important paradigm shift for EU policy, which traditionally emphasised cyber resilience from the position of economic impact, rather than defence.

The multidimensional warfare used in the ongoing armed conflict in Ukraine presents a complex security challenge. To this end, the purpose of this report is to analyse the magnitude of the cyber dimension of the war in Ukraine, its impact, and the lessons learned. The understanding gained through this report can be leveraged to better understand the threat environment, and strengthen cyber resilience and defence capabilities.

1.2 Structure

This report is structured into four substantive parts. The first section analyses the extent and impact of the cyber dimension in the war in Ukraine, including the risks and harms to the civilian population. It describes the role of cyber in this international armed conflict, and further details the types of cyberattacks and operations, their strategic importance, and observed trends in the use of cyber.

The second section dives into lessons learned based on the outlined evidence. This includes the participation of non-traditional actors engaged in cyberattacks of geopolitical relevance, the spill-over effect of cyberattacks deployed in connection to the war, the level of coordination between kinetic and cyber operations, and – importantly – the impact on and harm caused to the civilian population by cyberattacks and operations.

The third section elaborates on the short- and long-term impacts of the hostilities waged against Ukraine, including the policy, legal, and strategic implications, the potential impact for other existing or future armed conflicts, and the implications for the EU's CSDP missions.

The concluding section builds on the earlier analytical parts of the report, and proposes evidence-based recommendations with relevance to the EU institutions, and especially EU lawmakers. This part consists of an overview of key trends and challenges, coupled with proposals and suggestions that address them.

[1] N.B. The military invasion in Crimea, Donetsk and Luhansk regions in 2014.

[2] Council of the European Union, 'A Strategic Compass for a stronger EU security and defence in the next decade', Press Release, 21 March 2022. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/.

1.3 Methodological approach and data

This report builds on the authors' expert understanding of the issues pertaining to the role of cyber in the ongoing war between the Russian Federation and Ukraine, its impact on critical infrastructure, and lessons learned for the future use of cyber means in armed conflicts. This expert knowledge, including previous highly relevant research, forms the basis for further detailed and targeted desk research that includes academic and non-academic sources and additional interviews with practitioners. Two semi-structured individual interviews were conducted to complement our analysis. The interviewees were representatives from the European External Action Service (EEAS) and the State Service of Special Communications and Information Protection of Ukraine.

The report relies on extensive data collected by the CyberPeace Institute in the context of the Russian war against Ukraine. Since February 2022, the CyberPeace Institute has been documenting cyberattacks and operations affecting critical infrastructure essential for the survival of the civilian population and civilian objects, including attacks in non-belligerent states. This information is publicly available on the Cyber Attacks in Times of Conflict Platform #Ukraine[3]. The CyberPeace Institute also prepares quarterly analysis reports[4] that provide observations related to the cyber dimensions of the war. These reports combine analysis of data collected in the Cyber Attacks in Times of Conflict Platform #Ukraine and information gathered through open-source intelligence (OSINT) research. The collected evidence is independently analysed in the Institute to outline the trends and emerging issues relating to cyber incidents taking place in Ukraine, the Russian Federation and other, non-belligerent countries impacted by cyberattacks related to this conflict.

[3] CyberPeace Institute, 'Cyber Attacks in Times of Conflict Platform #Ukraine'. Available at: https://cyberconflicts.cyberpeaceinstitute.org/.

[4] CyberPeace Institute, Quarterly Analysis Report - Q3 July to September 2022, May 3, 2023. Available at: https://cyberpeaceinstitute.org/news/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q1-2023/; CyberPeace Institute, Quarterly Analysis Report - Q4 October to December 2022, February 1, 2023. Available at: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q4-2022/; CyberPeace Institute, Quarterly Analysis Report - Q1 January to March 2023, December 16, 2022. Available at: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2022/.

2 Cyber dimension of the war in Ukraine

2.1 Role of cyber in the Russian war of aggression against Ukraine

The use of cyberattacks and operations in peacetime and during armed conflicts is today a reality. The February 2022 territorial invasion of Ukraine by the armed forces of the Russian Federation was accompanied by destructive cyberattacks, and clearly demonstrates this trend[5]. The use of cyberattacks as a means of warfare has also been observed before between states including the Russian Federation and Georgia, Israel and Iran, and the Russian Federation and Ukraine (with Russia deploying cyberattacks against Ukraine since 2014, in particular). The CyberPeace Institute has been documenting cyberattacks on critical infrastructure and civilian objects since the beginning of the Russian war of aggression against Ukraine[6]. The documentation of attacks contributes to the analysis of the use of cyber means in wartime. As of 31 May 2023, the Institute recorded 1 998 cyberattacks and operations perpetrated by 98 different actors. These cyber incidents targeted 23 different critical infrastructure sectors, affecting Ukraine, the Russian Federation, and some 49 other countries.

This body of data shows that the volume and scope of cyberattacks against Ukraine have been very high, and would have drawn much more attention under different circumstances (if there were not kinetic attacks). Observed attacks are not innovative with respect to the technology or methods employed, but the number of attacks, the perpetrators, and the use of cyber against critical infrastructure are cause for alarm. Moreover, connections between different types of attacks have been observed. Cyberattacks and operations are now an established type of military operation, and are being coordinated with, or synchronised around, kinetic military operations. It is this combination of kinetic and cyberattacks that is having such a profound impact on the civilian population, affecting critical infrastructure and civilian objects that they depend upon, including the information space. This combination is disruptive and destabilising.

In the context of military hostilities such as the war in Ukraine, it is the use of conventional weapons that currently achieves a larger visible and more measurable impact. Yet, as outlined by Christian-Marc LIFLANDER, Head of the Cyber and Hybrid Policy Section's (CHP) Emerging Security Challenges Division (ESC) at NATO: *'Unlike troop buildups or other forms of military mobilisation that are infrequent and highly visible, cyber operations are the result of operational cycles that occur covertly and continuously* ***through peacetime and wartime****. The targeting of sensitive networks during peacetime lets attackers lay the groundwork for malware intended for wartime use. The methods attackers use to establish initial footholds for espionage activities are indistinguishable from those that precede cyberattacks. For cyber units, war does not fundamentally change the way they prepare or start to fight'*[7].

Aggregated data collected and analysed by the CyberPeace Institute supports the observation that it is important to move beyond preconceived notions of the role that cyberattacks would play in wartime, and of the role they play in Russia's military operations.

Observations from use of cyber in other contexts support this. Malware wipers have been used heavily during the conflict with a view to destroying and encrypting data and systems. For example, the attack on the Viasat satellite network resulted in internet access being cut off for more than two weeks. Nearly

[5] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, 22 June 2022. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[6] The war between Ukraine and the Russian Federation has witnessed a prolific use of cyber, and the CyberPeace Institute has been monitoring and aggregating data in a publicly available platform since the beginning of 2022 with regard to cyberattacks and operations against critical infrastructure and civilian objects. Access the Cyber Attacks in Times of Conflict Platform #Ukraine here: https://cyberconflicts.cyberpeaceinstitute.org/.

[7] Keynote address at the Geneva Press Club organised by the CyberPeace Institute: 'What lessons can be learned from the use of cyber in 21st century conflicts?', 13 October 2022.

9 000 subscribers of a satellite internet service provider were deprived of the internet in France. Around a third of 40 000 subscribers of another satellite internet service provider in Europe were affected, and a major German energy company has lost remote monitoring access to over 5 800 wind turbines. A malware wiper attack on 25 February 2022 against a border control station slowed the process of allowing refugees crossing into Romania.

Cyberattacks with disruptive elements have led to the obstruction of access to telecommunications and internet services, limited access to money, interrupted access to news, and in the past have been shown to lead to denial of access to electricity, heating and water. For example, on 28 March 2022 an attack on Ukrtelecom led to a connectivity collapse to 13 % of pre-war levels, with nation-wide disruption observed. The spread of disinformation and propaganda, including through attacks on the media sector, are destabilising as they influence the information space and limit the population's access to timely, reliable and official information. This undermines trust in institutions through information manipulation. The compromise of data – data hacked and leaked, notably by hacktivist collectives – is leading to huge volumes of data on organisations and individuals being published online with unknown long-term implications.

Finally, it is important to underscore the importance of the effectiveness of cyber defence by Ukraine in repelling attacks, and/or mitigating their impact[8]. Ukraine bolstered the resilience of its national Information and Communication Technology (ICT) infrastructure and cyber incident response prior to and during the war, in cooperation with allied governments and private companies[9]. Ukraine's private sector has also largely contributed to this process[10]. This included activities to strengthen the cyber resilience of Ukraine prior to and since the 2014 and 2022 military invasions, and cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)[11]. Ukraine's preparation, recognising that it has been the subject of cyberattacks for many years, has involved private-public partnerships. With the outbreak of the war, private actors, such as Microsoft, Google, Amazon, and ESET, have publicly acknowledged the role played in terms of tracking and forecasting cyber threats[12], hosting of governmental data in the public cloud outside Ukraine, and other forms of collaboration by the Government of Ukraine to thwart cyber threats[13].

[8] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, 22 June 2022. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

[9] Susan Landau, 'Cyberwar in Ukraine: What You See Is Not What's Really There', *Lawfare*, 30 September 2022, https://www.lawfareblog.com/cyberwar-ukraine-what-you-see-not-whats-really-there.

[10] Emma Schroeder and Sean Dack, 'A parallel terrain: Public-private defense of the Ukrainian information environment,' *Atlantic Council*, 27 February 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/.

[11] State Service of Special Communications and Information Protection of Ukraine, 'Ukraine has signed an agreement on accession to the NATO Cooperative Cyber Defence Centre of Excellence', 19 January 2023. Available at: https://cip.gov.ua/en/news/ukrayina-pidpisala-ugodu-pro-priyednannya-do-ob-yednanogo-centru-peredovikh-tekhnologii-z-kiberoboroni-nato.

[12] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, 22 June 2022. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

[13] Gareth Corfield, 'Russian cyberattacks on Ukraine halved with help from Amazon and Microsoft', *The Telegraph*, 7 January 2023. Available at: https://www.telegraph.co.uk/business/2023/01/07/russian-cyberattacks-ukraine-halved-help-amazon-microsoft/;
Stephanie Pell, 'Private-Sector Cyber Defense in Armed Conflict', *Lawfare*, 1 December 2022. Available at: https://www.lawfareblog.com/private-sector-cyber-defense-armed-conflict;
Irene Sánchez Cózar and José Ignacio Torreblanca, 'Ukraine one year on: When tech companies go to war', *European Council on Foreign Relations*, 7 March 2023. Available at: https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/;
Jenna McLaughlin, 'Russia bombards Ukraine with cyberattacks, but the impact appears limited', *NPR*. 3 March 2023. Available at: https://www.npr.org/2023/02/23/1159039051/russia-bombards-ukraine-with-cyberattacks-but-the-impact-appears-limited.

2.2 Types of cyberattacks and operations

The Russian war of aggression against Ukraine demonstrates an important dynamic regarding cyber threats and new and emerging vectors and vulnerabilities. The cyberattacks and operations have been deployed with the aim to destroy data and systems, disrupt critical infrastructure and services, control the information space, exfiltrate significant volumes of data, conduct reconnaissance and espionage, and execute influence operations (including disinformation campaigns to break down trust in public information and institutions, create confusion, and discredit belligerents and their allies)[14].

Destructive attacks: Cyberattacks that aim for permanent deletion of data or damage to systems rendering them unrecoverable. These attacks can have long-lasting effects on organisations if they are unable to retrieve backups or reset systems. Examples include wiper malware targeting Ukrainian government entities and other sectors. A recent case included the reappearance of a destructive wiper malware dubbed 'CaddyWiper' that was discovered by the Computer Emergency Response Team of Ukraine (CERT-UA). The latest deployment of the wiper malware took place in January 2023 against Ukraine's National Information Agency 'Ukrinform'[15].

Disruptive attacks: Cyberattacks aiming to cause disruption of services and operations have featured heavily during the conflict, including on Ukrainian organisations during the early stages of the invasion, on Russian organisations following a call to civilians by the Ukrainian government, and on public institutions in some NATO member countries after public security or economic announcements. Distributed Denial of Service (DDoS) attacks have been the most prevalent types of attacks observed during this war, particularly affecting the public and financial sectors. DDoS attacks account for 87.5 % of all cyberattacks recorded by the CyberPeace Institute between January and March 2023. The financial, public and ICT sectors were targeted the most. A particularly harmful trend is the targeting of Ukrainian non-profit organisations, which are a vulnerable target due to their generally low preparedness and lack of resilience measures[16].

Data weaponisation: Cyberattacks leading to the theft or exfiltration of data or the acquisition of data for espionage, surveillance, or intelligence purposes. Although the latter are expected activities in cyberspace in the context of war and geo-politics, the former are attacks which have been heavily conducted by collectives of actors in the name of activism. Data relating to private and public organisations is being exfiltrated and published online at a pace rarely seen before. Data has been weaponised in hack and leak operations. A recent notable incident was discovered in March 2023 and attempted to target EU countries. A Russian state-sponsored threat actor sent spear phishing e-mails with information concerning the Polish Ambassador's visit to the United States. This campaign also used a method of mirroring real information exchange systems used by EU nations. The e-mails contained malware allowing the threat actor to drop files on the victim's machine and move through the victim's network to collect data[17].

Disinformation: Information operations based on disinformation and propaganda are not new methods of warfare, but the cyber domain has allowed for their deployment at an unprecedented speed and scale. Attacks with a focus on the spreading of false information and propaganda have featured in this armed conflict. Threat actors appear to be aiming to influence the information space and limit access to timely, reliable, and official information for the population, or purposefully confuse and undermine information

[14] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, 22 June 2022. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

[15] Ibid.

[16] Ibid.

[17] Ibid.

environments[18]. From SMS spam campaigns spreading false information about technical malfunctions of ATMs, to cyberattacks on TV stations in which information is falsely displayed on the news ticker or deep fake videos are streamed, and threat actors compromising e-mail accounts to gain access to the social media accounts of high-profile Ukrainians to post disinformation. In July 2022, for example, threat actors defaced a Ukrainian radio channel. The perpetrators played a voice saying that the Ukrainian President is in intensive care, and falsely claiming that the Chairman of the Verkhovna Rada would undertake the President's duties[19].

It is important to note that for the Russian Federation, 'information confrontation' or 'information warfare' is a broad concept and key enabler of its attempts to gain victory in current and future conflicts, and is not a separate function or domain from 'cyber'. As such, instead of 'cyberspace', Russia refers to 'information space'[20].

2.3 Trends in the use of cyber observed in the war of aggression against Ukraine

The Russian Federation has been observed to coordinate destructive and disruptive cyberattacks aimed at Ukraine, network penetration and espionage in targeted countries that are perceived as Ukraine's allies, and cyber-influence operations designed to influence people globally. The nexus between cyberattacks and the proliferation of harmful content online, including disinformation, creates a convergence that presents unique risks to populations worldwide and increases the human impact of cyber threats on vulnerable communities.

The damaging and destabilising impacts of the use of cyber in the war in Ukraine are exacerbated by the large-scale participation of non-traditional and non-state actors, including state-backed hackers and patriotic amateurs or volunteers, in a domain that traditionally sees an exclusive engagement of states. The lowering of the threshold to enter the cyber domain complicates possible legal responses to cyberattacks – blurring the lines between politically motivated cyber operations and cybercrime, for example, in cases of ransomware attacks by cybercriminal groups claiming allegiance to a belligerent country.

The impact of cyber in this Russian war of aggression against Ukraine first and foremost affects people in Ukraine, especially as cyberattacks and operations have been coordinated with kinetic attacks. However, cyberattacks are also being carried out against targets beyond the territorial borders of the two belligerent countries, which is compounded by the interconnectivity inherent in cyberspace. The spill-over effect of cyberattacks combined with the wide range of attackers means that virtually any country, company, or organisation can be impacted.

Critical infrastructure has been a regular target in this war. As all essential services now largely depend on ICT and the elaboration and transmission of information online, there is a pronounced economic and operational impact on organisations and governments that are targeted. Cyberattacks and operations targeting critical infrastructure can have severe impacts on the civilian population, and can take an immense toll on human security, causing harm to affected individuals and communities.

[18] OECD, 'Disinformation and Russia's war of aggression against Ukraine', 3 November 2022. Available at: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/.

[19] CyberPeace Institute, 'Quarterly Analysis Report - Q3 July to September 2022', 3 May 3 2023. Available at: https://cyberpeaceinstitute.org/news/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q1-2023/.

[20] See for example: Handbook of Russian Information Warfare, Keir Gilles, Research Division, NATO Defense College, November 2016.

3 Lessons learned

3.1 Connecting kinetic and cyber operations

The Russian Federation has been observed to coordinate cyberattacks and conventional weapons to inflict maximum harm on Ukraine and its population. For example, malware identified on 23 February 2022 by Microsoft was launched against computers in Ukraine hours before the invasion. Around the same time, Russian cyberattacks disabled modems that communicate with commercial satellite communications networks (Viasat Inc's KA-SAT) to disrupt Ukrainian command and control during the invasion[21]. Other cyberattacks during the conflict targeted government networks and other critical infrastructure before the deployment of kinetic attacks[22].

At a tactical level, cyberattacks provide advantages when combined with conventional weapons. For example, a cyberattack can disable or confuse command networks, so kinetic attacks can target with higher effectiveness. Coordinating cyber and kinetic actions requires a high degree of planning, and the timing of some cyber operations deployed by the Russian Federation suggests they were intended to support conventional operations[23].

The use of conventional weapons in combination with cyber operations targeting critical infrastructure amplifies the risks to, and harm inflicted on, the civilian population. By July 2022, Russia had focused on inflicting damage to the civilian population through a combination of cyber and kinetic attacks – for example, by targeting energy infrastructure during the winter[24]. Ukraine's largest private energy company, DTEK, was hacked with the presumed aim of destabilising its technological processes, while simultaneously the thermal power plant of the same company was shelled[25]. The deliberate targeting of critical civilian infrastructure essential to populations has profoundly changed the security environment, including beyond the borders of the two belligerent states[26].

3.2 Participation of non-traditional actors engaged in cyberattacks

The use of cyber in the Russian war against Ukraine has been shaped by the large-scale participation of non-state actors. Due to the lowering of the threshold to conduct attacks, nation state actors are no longer the only ones with offensive capabilities. In addition, both belligerents called for support of persons willing to join a 'cyber army' in the early days of the hostilities. The threat landscape now includes nation states, nation state affiliated actors, collectives and hacktivists, and cybercriminal groups.

The CyberPeace Institute has recorded cyberattacks and operations perpetrated by 98 different threat actors, as of 31st May 2023. Of all the cyberattacks analysed by the Institute, some 80 % are 'self-attributed'

[21] U.S. Department of State, 'Attribution of Russia's Malicious Cyber Activity Against Ukraine', Press Statement, 10 May 2022. Available at: https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/.

[22] Microsoft, 'Defending Ukraine: Early Lessons from the Cyber War', 22 June 2022. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

[23] James Andrew Lewis, 'Cyber War and Ukraine', 16 June 2022. Available at: https://www.csis.org/analysis/cyber-war-and-ukraine.

[24] Economic Security Council of Ukraine (ESCU), 'Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions', 17 January 2023. Available at: https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-17-Ukraine-ESCU-Cyber-Artiller-Propaganda- Comprehensive-Analysis-of-Russian-Warfare-Dimensions-ESCU.pdf.

[25] Victor Zhora, Twitter, 1 July, 2022. Available at: https://twitter.com/VZhora/status/1542858906560512000?lang=en; CyberSecurity Connect, 'Russian Hackers Blamed for Cyber Attack on Ukrainian Energy Firm DTEK Group', 8 July 2022. Available at: https://www.cybersecurityconnect.com.au/critical-infrastructure/8008-russian-hackers-blamed-for-cyber-attack-on-ukrainian-energy-firm-dtek-group.

[26] CyberPeace Institute and Charlotte Lindsey, 'Ukraine conflict: One year of cyberattacks and operations', 24 February 2023. Available at: https://cyberpeaceinstitute.org/news/ukraine-conflict-one-year-anniversary.

attacks, in which threat actors publicly disclose a cyberattack and attribute themselves as the actor behind the attack[27]. This aspect further points to the probable geopolitical importance of these attacks. For example, KillNet, a hacktivist group affiliated with Russia, conducted DDoS attacks against healthcare facilities in countries that align with Ukraine[28].

The cyber domain is enabling a range of actors to conduct attacks affecting both belligerent and non-belligerent states. The government-initiated volunteer 'cyber army' has become a notable pro-Ukrainian threat actor. Initiated by the Ukrainian government, the IT Army of Ukraine is a less conventional player whose DDoS attacks are heavily impacting Russian online resources[29]. On 26 February 2022, the Ministry for Digital Transformation of Ukraine announced the call for an army of IT specialists to fight for Ukraine in cyberspace[30] [31].This call was unique for a State in a situation of armed conflict and aimed to attract Ukrainian talent to 'continue the fight on the digital front'. Whilst addressed to Ukrainians, in the context of the global outcry against Russia's invasion and military attacks on civilians, and the interconnected and open nature of the Internet, the call has likely resulted in the participation of people from all over the world[32].

The participation of loosely affiliated actors in deploying cyberattacks during an armed conflict poses several challenges, and sets a dangerous precedent for any future conflicts. Participation by actors not part of the belligerent armed forces blurs the lines on the status of such actors. International Humanitarian Law (IHL) makes a clear distinction between civilians and military armed forces and provides modalities on what it means for a person to participate directly or indirectly in an armed conflict. Civilians directly participating in hostilities may lose their protection as civilians accorded under IHL, and could be targeted by cyber or kinetic means, and/or for prosecution. This extends the potential impact of conflict on individuals and societies[33].

Loosely organised groups without proper coordination, training, and rules of engagement can cause direct harm and impact via second and third order consequences of the attacks they are engaging in. Participation by such actors in hostilities also poses attribution challenges. The technical attribution must differentiate between perpetrators, which can be difficult, especially if their tactics, techniques, and procedures (TTPs) are shared among criminals and proxies. This makes it more difficult to determine the

[27] The Institute does not conduct its own attribution of incidents to identify the actor(s) involved, but documents the attribution efforts by others to link a particular individual, group or state to a specific incident. As there is a reliance on publicly available data, the data on documented cyberattacks in the Cyber Attacks in Times of Conflict #Ukraine Platform gives a classification of certainty based on the reliability of the information source. See the Data and Methodology section of the Platform. Available at: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology.

[28] Computer Weekly, 'Russian DDoS hacktivists seen targeting western hospitals', 31 January 2023. Available at: https://www.computerweekly.com/news/365529957/Russian-DDoS-hacktivists-seen-targeting-western-hospitals.

[29] Stéphane Duguin and CyberPeace Institute, 'How an armed conflict is destabilizing cyberspace for us all', 11 November 2022, Available at:
https://cyberpeaceinstitute.org/news/how-armed-conflict-is-destabilizing-cyberspace/.

[30] Olena Roshchina, 'Minister Fedorov: We are creating an IT Army,' *Ukrainska Pravda*, 26 February 2022, https://www.pravda.com.ua/eng/news/2022/02/26/7326225/.

[31] Emma Raffray, 'Ukraine: 100 days of war in cyberspace', 2 June 2022, Available at: https://cyberpeaceinstitute.org/news/ukraine-100-days-of-war-in-cyberspace/.

[32] Stéphane Duguin and Raj Samani, 'Ukraine: Cyber and Participation in Hostilities', *CyberPeace Institute*, 7 March 2022. Available at: https://cyberpeaceinstitute.org/news/cyber-and-participation-in-hostilities/.

[33] According to the International Committee of the Red Cross (ICRC) 2009 Interpretative Guidance on Direct Participation in Hostilities, 'Persons take a direct part in hostilities when they commit acts aimed at supporting one party to the conflict by directly causing harm to another party, either by directly inflicting death, injury or destruction, or by directly harming the enemy's military operations or capabilities. If and for as long as civilians commit such acts, they take a direct part in hostilities and lose their protection against attack'. Available at: https://www.icrc.org/en/publication/0990-interpretive-guidance-notion-direct-participation-hostilities-under-international.

actual perpetrator. The plausible deniability of the attacker's identity means that there is a low risk of retaliation for cyberattacks, while at the same time, possible misattribution increases the risk of miscalculation and potential retaliation in conventional domains, which can escalate the conflict.

The technical threshold between cybercriminal groups and nation state actors is also getting closer, while 'off the shelf malware' and other tools are becoming more accessible. There have also been cases where threat actors have hijacked the infrastructure of unsuspecting parties or other threat actors – for example, in false flag operations that further complicate adequate response. The obstacles in technical attribution can, in turn, complicate accountability for harm caused by cyberattacks. This contributes to the destabilisation of cyberspace, and raises important policy and legal challenges[34].

3.3 Spill-over effect of cyberattacks deployed in connection to the Russian war of aggression against Ukraine

The abovementioned cyberattack accompanying the launch of the invasion that disabled modems that communicate with Viasat Inc's KA-SAT satellite network is such an example. The incident led to an interruption in the supply of internet access to people and companies in both Ukraine and many countries across Europe. Owing to the interconnection of telecommunications systems, the attack was aimed at the government and military objects within Ukraine, and resulted in impact on the civilian population and civilian objects in Ukraine and beyond, including loss of internet access and disruption to systems in the energy sector[35]. While primarily the attack impacted the Ukrainian civilian population, so they were not able to access reliable information from the government during the conflict, secondarily, civilians in other EU countries experienced internet outages as a spill-over effect of the attack outside of the conflict zone. This incident shows that a cyber operation against a specific system may have repercussions on various other systems, regardless of where those systems are located.

Both the targeting of critical infrastructures and the spill-over effects on civilians not directly involved in the conflict are undermining the rules-based international order anchored in the framework of responsible state behaviour in cyberspace. The EU and the *Five Eyes* governments released public statements attributing AcidRain to the Russian military intelligence (GRU) and linking it to other types of destructive wiper malware that had been used to target the Ukrainian government and private sector networks. Further specific national statements aligning with this attribution were made by a number of individual EU Member States. This consistent response by many governments is an important step in the practice of political attribution of cyberattacks, and contributes to the development of established states' practice[36].

3.4 The impact of cyberattacks and operations on the civilian population

The use of cyberattacks and operations as part of the war in Ukraine has an important human component. Such attacks may expose the civilian population and critical civilian infrastructure to harm, as essential services for society and economies depend on such infrastructure. Furthermore, cyber operations add

[34] Stéphane Duguin and Raj Samani, 'Ukraine: Cyber and Participation in Hostilities', *CyberPeace Institute*, 7 March 2022. Available at: https://cyberpeaceinstitute.org/news/cyber-and-participation-in-hostilities/.

[35] CyberPeace Institute, 'Case Study: Viasat', June 2022. Available at: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

[36] Ibid.

another layer of uncertainty in terms of the harm to populations, as the impact on victims can, in some cases, materialise only after a time delay, or may be indirect, but cause harm[37].

Destructive attacks, such as the deployment of wiper malware targeting Ukrainian entities and organisations, can lead to the deletion of data or damage to systems, rendering them unrecoverable. An example was the wiper attack on a border control station on 25 February 2022, which was reported to have slowed the process of enabling refugees to cross into Romania[38].

Disruptive attacks lead to the interruption of services and operations. These types of attacks have been particularly hard-felt by sectors related to critical infrastructure – such as public administration, energy, ICT, and finance – impacting the connectivity and availability of vital services.

Data weaponisation attacks aim to steal/exfiltrate or acquire data for espionage, surveillance, or intelligence purposes. This includes hack and leak attacks through the theft and leak of data for political or ideological purposes. The leak of data and information from institutions and organisations sows distrust, demonstrates an inability to secure sensitive data, and potentially places individuals at risk. Although the latter are known practices in the context of war and geopolitical conflicts, the former are attacks which have been heavily conducted by collectives of actors in the name of activism. Data relating to private and public organisations is being exfiltrated and published online at a pace rarely seen before. For example, in an alleged hack and leak operation against a Ukrainian administrative centre the leaked data contained personal identifiable information of Ukrainian citizens[39].

Disinformation or propaganda can lead to the spread and circulation of false information, and limit access to timely, reliable, and official information for the population. Threat actors appear to be trying to influence information circulated through mainstream media, defacing websites or altering information through cyberattacks to spread geopolitical messages, spread disinformation, and influence public opinion. Disinformation can drive secondary impacts of the war, which can heighten the risk of misunderstandings, conflict, violence, human rights violations, and mass atrocities.

[37] CyberPeace Institute and Charlotte Lindsey, 'Ukraine conflict: One year of cyberattacks and operations', 24 February 2023. Available at: https://cyberpeaceinstitute.org/news/ukraine-conflict-one-year-anniversary.

[38] Kyle Alspach, 'Ukraine border control hit with wiper cyberattack, slowing refugee crossing', *VentureBeat*, 27 February 2022. Available at: https://venturebeat.com/security/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/.

[39] CyberPeace Institute, 'Quarterly Analysis Report - Q3 July to September 2022', 3 May 2023. Available at: https://cyberpeaceinstitute.org/news/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q1-2023/.

4 The short- and long-term impacts of the Russian war of aggression against Ukraine

4.1 Policy, legal, and strategic implications

The use of cyber means and information operations in peacetime and wartime raises serious challenges for public and private actors regarding the rules and regulations applicable to cyberattacks. Cyberattacks and operations do not happen in a legal vacuum.

Two UN processes on responsible behaviour (the Open-Ended Working Group and the UN Group of Governmental Experts) led to states reaffirming their agreement that international law applies to cyberspace.

The applicable body of international law, particularly the UN Charter, IHL, and Human Rights Law, is extremely relevant in times of international armed conflict. International law offers protection against the potential human cost of cyber operations, and IHL especially ensures protection for civilians and civilian infrastructure, and aims to reduce suffering.

However, the reality of the use of cyber against critical infrastructure raises serious concerns regarding how states respect and abide by the existing legal framework. Cyber operations are not, per se, 'illegal' under international law, but may be regarded as such if they produce effects that violate international law obligations. A critical gap is the lack of agreement on how international law applies. The remaining challenges associated with the applicability of international law in cyberspace lead to exploitation of these uncertainties.

To close this gap, states must agree on clear rules for their responsibility under IHL, outlining how these principles apply to the use of ICT and to operations in the context of armed conflicts. These clarifications should also consider the Rome Statute, which is particularly relevant for the involvement of non-traditional actors, as it imposes the duty of every state to exercise its criminal jurisdiction over those responsible for international crimes. There are several ways we can work towards building a common understanding regarding accountability for the malicious use of cyber, including via statements of governments and state practice. States can also actively clarify how international law was breached, for example, when sanctions are imposed or when political attributions are made.

Furthermore, current policy and legal responses require further clarification, or fall short of effectively addressing these challenges for several other reasons. For example, cyber tools may serve as dual-use technology for military and civilian purposes, which adds an additional layer of complexity. The non-exhaustive list of needed clarifications includes establishing what constitutes an 'attack', 'harm', 'object', 'military objective', and 'criminal responsibility' in cyberspace, and the lack of consensus on the specific responses to different types of attacks. Moreover, rules of peacetime international law that are primarily challenged during malicious cyber operations include the concepts of sovereignty, due diligence, and non-intervention, and it is important to clarify their scope in cyberspace.

4.2 Potential impact for other existing or future armed conflicts

To date, cyber operations by themselves do not guarantee the achievement of strategic objectives in armed conflicts. The means and methods of cyber use in the war in Ukraine can be indicative of the approaches that could be used in future armed conflicts, as this conflict has been a test kitchen for both the offensive and defensive use of cyber. Cyberattacks, information operations, and kinetic attacks are intrinsically connected in current and future warfare. This connection is key to understanding coordinated attacks in Ukraine, their impact on several sectors of critical infrastructure, and cyber-influence operations that target diverse audiences, including beyond belligerent countries. Cyberspace is further destabilised by the large-scale participation of non-traditional actors. A defining aspect in the Russian war of aggression against Ukraine has been to inflict harm on the civilian populations.

It will be important to learn lessons from this armed conflict, and to ensure that there is appropriate accountability for breaches of international law, including holding the perpetrators of violations liable for their actions. Moreover, once the active hostilities cease, it will be important to determine how cyber has been used to violate international law.

Other technological challenges emerge in the background of the war and can influence existing and future conflicts, including the proliferation of marketplaces for zero-day exploits, systemic effects of vulnerabilities in widely used open-source software, specific threats posed by commercial ransomware[40], and tools that can enable new modalities of cyber operations, such as the use of large language models and generative Artificial Intelligence (AI) that increases the capacity to carry out cyberattacks and operations. These tools further decrease the threshold for actors to participate in conflicts.

4.3 Implications for CSDP missions

CSDP is a key pillar of the EU Strategic Compass toward strengthening the bloc's security and defence policy. Throughout CSDP missions, the EU leverages bilateral support with the aim of enhancing the resilience of the security sector of the respective countries, including cybersecurity, countering disinformation, and other coordinated information operations. This work aims to augment domestic cyber resilience, while placing the civilian aspect into national security as part of a comprehensive security approach. This support is especially relevant considering the regional dimension of the war in Ukraine, both for the EU member countries themselves, and for the CSDP missions, given that an unsecured neighbour poses a threat to the security of Member States.

In reaction to the war in Ukraine, in June 2022, the European Parliament adopted a resolution on security in the Eastern Partnership (EaP) and the role of the common security and defence policy, which is calling on the EU '*to expand support mechanisms for the further participation of the EaP countries in CSDP civilian and military missions and operations*'[41]. The cyber resilience of CSDP missions and operations needs to respond to the lessons learned from the ongoing war in Ukraine. Defending against a multidimensional military invasion requires coordinated and comprehensive strategies to strengthen defences against a range of destructive and disruptive cyberattacks, data infiltration and leaks, and influence operations using propaganda, disinformation, and fake news. Cyber-influence operations are especially well positioned to have far-reaching impact beyond belligerent countries, as they take advantage of the longstanding openness of democratic societies, and the public polarisation that is characteristic of today's societies. Reacting to these challenges, the CSDP Partnership Mission in Moldova, formally established on 24 April 2023 at the request of Moldova's authorities, was specifically designed to address hybrid warfare[42].

[40] Taylor Grossman, Monica Kaminska, James Shires, and Max Smeets, 'The Cyber Dimensions of the Russia-Ukraine War', *European Cyber Conflict Research Initiative (ECCRI)*, April 2023. Available at: https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf.

[41] European Parliament, 'Security in the Eastern Partnership area and the role of the common security and defence policy', European Parliament resolution of 8 June 2022 on security in the Eastern Partnership area and the role of the common security and defence policy (2021/2199(INI)), 8 June 2022. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0236_EN.pdf.

[42] Council of the European Union, 'Moldova: EU launches civilian mission to strengthen the resilience of the security sector in the areas of crisis management and countering hybrid threats,' Press Release, 22 May 2023, Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/05/22/moldova-eu-launches-civilian-mission-to-strengthen-the-resilience-of-the-security-sector-in-the-areas-of-crisis-management-and-countering-hybrid-threats/.

Increased cyber resilience and defence necessitates a more coordinated training, planning, and implementation process between EU actors and the host countries of CSDP missions and operations. A targeted approach towards the countries should look into recent technological advances, as well as the lessons learned from protecting critical information infrastructure. While some measures can be adopted across the missions, each set of activities must be needs- and context-driven to correspond with the needs and realities of the missions, while fitting into the larger existing EU ecosystem. The EU should also explore different options in terms of how to support the counties across the existing measures and capacity building programmes that are already in place – for example, through advancing mechanisms of political messaging and signalling, sanctions against the perpetrator, and including diplomacy streams in cybersecurity capacity building. The European Peace Facilities (APF) Assistance Measures are well-positioned to provide such assistance and have been used to strengthen the resilience of Ukraine, Georgia and Moldova to counter hybrid threats, including cyberattacks[43].

Recent advances in cyber threat intelligence and end-point protection have helped Ukraine withstand a high percentage of destructive and disruptive cyberattacks. Extending cooperation in the domain of cyber threats must include the work of all relevant actors to analyse the threat landscape and evolution of cyber conflicts, and to increase resources on cybersecurity awareness initiatives. Two immediate considerations for increased cyber resilience and defence reflecting on the Ukrainian successful model of cyber defence are prioritisation of public private partnerships and the cross-border protection of a country's data assets against cyber or kinetic attacks. Additionally, communication and timely information sharing about cyber threats and vulnerabilities between and among states, as well as between the public and private sector is essential to ensure better preparedness and that preventive action can be taken before threats occur, rather than after an event has taken place. Preparedness and partnerships in cybersecurity developed since 2014 have been key for Ukraine's cyber defence.

Under the EU's Permanent Structured Cooperation **(PESCO) Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRTs)** project, the EU is able to pool together the cybersecurity capacities of Member States and provide support upon request. The EU has activated its CRRTs to support Ukraine's cyber-defence for the first time in an operational context, following a request from the Ukrainian government a week prior to the invasion in February 2022[44]. The CRRTs project will also be deployed to

[43] EU adopted two assistance measures under the European Peace Facility that will contribute to strengthening the capabilities and resilience of the Ukrainian armed forces and protecting the civilian population against the ongoing military aggression; whereas the assistance measures, worth EUR 1,5 billion in total, will finance the provision of equipment and supplies to the Ukrainian armed forces, including lethal equipment for the first time. European Parliament resolution of 8 June 2022 on security in the Eastern Partnership area and the role of the common security and defence policy (2021/2199(INI)),
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOC_2022_493_R_0007 ; On 4 May 2022, the Council of the European Union adopted two assistance measures under the European Peace Facility (EPF) in support of the Armed Forces of the Republic of Moldova and the Georgian Defence Forces. Moldova will receive EUR 40 million and Georgia will receive EUR 40 million over a period of 36 months to finance non-lethal equipment, supplies and services, including training and cyber-defence equipment. Council of the European Union, 'European Peace Facility: Council adopts assistance measures to support the defence sector of the Republic of Moldova and Georgia', Press Release, 4 May 2023, Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/05/04/european-peace-facility-council-adopts-assistance-measures-to-support-defence-sector-of-the-republic-of-moldova-and-georgia/?utm_source=dsms-auto&utm_medium=email&utm_campaign=European+Peace+Facility%3a+Council+adopts+assistance+measures+to+support+the+defence+sector+of+the+Republic+of+Moldova+and+Georgia.

[44] The European Parliament resolution of 8 June 2022 recognised that the EU's strategic interest can encompass inclusion of associated EaP countries (namely Ukraine, Moldova and Georgia) in individual PESCO projects, especially in the areas of hybrid threats and cybersecurity. The resolution called for exploring options to foster the cyber-capabilities of EaP countries, and proposed to launch civilian cyber missions. Regarding the European Union Advisory Mission (EUAM) in Ukraine, the resolution called for the extension of its mandate to cover combating hybrid threats, strategic communication, digital technology and cybersecurity. European Parliament resolution of 8 June 2022 on security in the Eastern Partnership area and the role of the

other members of the European Policy Community (EPC) as agreed during the EPC in Moldova on 1 June 2023.

The EU has formulated and is implementing legislation to increase its cyber resilience (overview in Section 4). Initiatives such as **Network and Information Security Directive** serve as an example for candidate countries that seek to align their legislation with acquis, including Ukraine and Moldova. The EU has provided support to create a national **cybersecurity law of Moldova** that will enter into force on 1 January 2025. The law was drafted taking into account the best practices from the EU legislation, which will facilitate regional and international communication and help enhance security and resilience of the Moldova cyber space. The support to the drafting of the Cybersecurity Law was provided by the Estonian e-Governance Academy's (eGA) experts within the EU European Peace Facility funded Moldova Rapid Assistance Project[45].

The CSDP aims for the EU to take a leading role in peacekeeping and conflict prevention. To further increase the civilian missions' effectiveness, Member States agreed on a new Civilian Compact within the framework of CSDP[46]. As such, it should undertake concrete measures to promote cyberpeace, based on the understanding of threats posed by cyberattacks and operations in the context of geopolitical tension and armed conflict. This information should be made available to the public to inform not only states, but also industry, academia, and civil society actors involved in capacity building initiatives, such as the CSDP civilian capacity development missions. Simultaneously, it is important to develop capabilities for measuring the harm and impact of cyberattacks, without which no recourse to accountability and justice is possible.

common security and defence policy (2021/2199(INI)) Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOC_2022_493_R_0007.

[45] Delegation of the European Union to the Republic of Moldova, 'Moldova adopted the EU-backed Cybersecurity Law', Press Release, 25, 11 May 2023, Available at: https://www.eeas.europa.eu/delegations/moldova/moldova-adopted-eu-backed-cybersecurity-law_en?s=223.

[46] European External Action Service, 'Launching the new Civilian CSDP Compact: Strengthening the EU's civilian response to crises and conflicts', Press Release, 25 May 2023. Available at: https://www.eeas.europa.eu/eeas/launching-new-civilian-csdp-compact-strengthening-eu%E2%80%99s-civilian-response-crises-and-conflicts_en.

5 Recommendations

5.1 Overview of key trends and challenges

Cyberspace has become a place of confrontation between states and also non-traditional actors. It is considered a new domain of warfare, like air, land, sea, and outer space. This has been acknowledged by NATO, which recognised cyberspace as a domain of military operations in 2016. Member States are also strengthening their understanding of the implementation procedures and scenario-based exercises for mutual assistance and/or solidarity, in line with Article 42(7) of the Treaty on European Union (TEU) and Article 222 of the Treaty on Functioning of the European Union (TFEU). The EU Strategic Compass[47] recognises cyber as a domain of warfare. Moreover, an increasing number of states are developing military cyber capabilities, and their use in both offensive and defensive activities is set to increase[48].

While the full scale and impact of cyberattacks and operations connected to the Russian war of aggression against Ukraine are still being gauged and determined, the early lessons demonstrate the importance of increasing the protection of critical civilian infrastructure that provides essential services to the public. The ongoing war against Ukraine offers important observations and considerations for enhancing the EU's understanding of the cyber dimensions relevant to a Member State's resilience in the cyber domain, such as the scope of the harm and damage, lessons learned, and the importance of multi-stakeholder efforts.

Important takeaways in relation to the ongoing war in Ukraine include the observed escalation of cyberattacks and operations that have included the participation of collectives with an allegiance to belligerent countries. This leads to civilianisation and crowdsourcing of war which has important legal considerations in relation to belligerency, and the direct and indirect participation in hostilities. De-escalating the cyber dimension of the conflict will be difficult even if there is an agreed cessation of hostilities and/or ceasefire, as monitoring the cyber dimensions of such a cessation or ceasefire will be very difficult. Additionally, the cyber dimension increases in complexity with the nexus between kinetic military action, cyberattacks and proliferation of harmful content[49]. Additionally, beyond the two belligerent countries, the spill-over effect of cyberattacks against non-belligerent countries has been notable. The full scale of such attacks is difficult to gauge unless there is a self-attribution by the threat actor, identification of the allegiance to one of the two belligerent countries, and proof of the intent behind these attacks. Importantly, cyberattacks and operations have been targeting a vast spectrum of entities. It is key to understand which organisations, networks, and systems have been negatively affected in order to direct recovery efforts to where there is the most need – for example, recovery from wiper malware attacks deployed for destructive purposes. There will also be impacts from some attacks that may only manifest themselves over time and require recovery years later, such as possible repercussions from the compromise and theft of data – for example, from a nuclear safety organisation.

Previous and ongoing investment efforts outlined above have enabled the resilience of Ukraine's ICT. It is important to understand and learn from the measures that contributed to this resilience to ensure future investments and collaboration to reinforce this capability. Finally, for years, external stakeholders have contributed to Ukrainian resilience efforts in cyberspace, and amplified the impact of these efforts through collaboration. Governments, the private sector, NGOs, and individual experts helped Ukraine become more

[47] Council of the European Union, 'A Strategic Compass for a stronger EU security and defence in the next decade', Press Release, 21 March 2022, Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/.

[48] Kubo Mačák and Laurent Gisel, Grammar: Rules in a cyber conflict, *European Union Institute for Security Studies (EUISS)*, November 2022. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_176.pdf.

[49] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, 22 June 2022. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

resilient to cyberattacks. Multi-stakeholder participation in discussions about recovery efforts is important to inform resource allocation, share experiences from the implementation of previous projects in Ukraine, and support the response to challenges posed by the impact of war on ICT.

The Russian war of aggression against Ukraine stressed the need to strengthen cyber defence capabilities through joint cooperation by Member States. This includes reducing the EU's strategic dependencies in critical cyber technologies and strengthening the European Defence Technological and Industrial Base (EDTIB). Cybersecurity threats have increased with respect to their scope, frequency and sophistication. Going towards a Zero Trust approach in regard to critical cyber technologies can support the EU's collective defence by minimising the potential vulnerabilities and the impact of evolving threats. The Zero Trust approach also aligns with GDPR principles by limiting access to sensitive data and ensuring higher standards of authorising users.

Increasing understanding of the threats to the EU's cybersecurity stemming from the present and potential use of cyber in armed conflicts and peacetime necessitates a human-centric, law- and human rights-based approach. It is vital to recognise the importance and scale of the harms and impacts on civilian populations that can be caused by the coordinated use of kinetic military operations and cyber operations in times of armed conflict, as well as the impact of cyberattacks beyond belligerent countries. Cyberattacks, information operations, and kinetic attacks are intrinsically connected in present and future warfare. This connection is key to understanding coordinated attacks in Ukraine, their impact on sectors of critical infrastructure, and cyber-influence operations that target diverse audiences, including beyond belligerent countries. Such coordination creates the need for a new approach that goes beyond addressing individual types of attacks and focuses on holistic cyber resilience, preparedness, and defence. Member States need to be able to counter coordinated threats with an evidence-based understanding of the threats, coordination between EU legislative efforts, and cooperation between research, governments, the private sector, civil society, and academia.

5.2 Suggestions and proposals for the EU

The EU has already proposed or implemented various projects and legislation to increase its cyber resilience[50]. The following brief overview will focus on selected recent initiatives that actively tackle or respond to the challenges presented by the current and emerging threats brought about by the cyber dimension of the war in Ukraine.

The war in Ukraine has significantly impacted the EU's foreign and defence policy, including their cyber dimension, and demonstrated that new approaches are necessary to bolster cyber resilience. The EU's cyber defence policy outlined in the Joint Communication on the EU Policy on Cyber Defence of 10 November 2022[51] and the Council Conclusions on the EU Policy on Cyber Defence published on

[50] Some of its initiatives include the European Union Agency for Cybersecurity (ENISA), created in 2004 and enhanced in 2019; the Directive on measures for a high common level of cybersecurity across the Union (the 'NIS2 Directive') which repeals the NIS Directive, entered into the force in January 2023; the European Parliament resolution of 13 June 2018 on cyber defence; the Resolution establishing the European Cybersecurity Industrial, Technology and Research Competence Centre, adopted in 2021; the Cyber Resilience Act 2022; the Negotiating mandate on the proposal for a regulation on the Union secure connectivity programme for the period 2023-2027, adopted by the Council in 2022; the Council's position on a draft regulation aimed at ensuring a high common level of cybersecurity across the EU institutions, bodies, offices and agencies, adopted in 2022; PESCO's various projects – in particular, the EU Cyber Rapid Response Team (CRRT), which was deployed for the first time at the beginning of the war in Ukraine; the installation of 'Security Operations Centers' (SOCs) that could be likened to 'police officers' in the digital world; and the Joint communication to the European Parliament and the Council on the EU Policy on Cyber Defence of 10 November 2022.

[51] European Commission, 'Cyber Defence: EU boosts action against cyber threats', Press Release, 10 November 2022, Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642.

22 May 2023[52] addresses the deteriorating security environment. This is done by placing the emphasis on enhancing cooperation and investments in cyber defence, closing the remaining cyber capabilities gaps, and strengthening relations between military and civilian actors. Considering the lessons learned in Ukraine, close civilian-military cooperation is needed, including with academia, civil society and the private sector. Elaboration of such cooperation mechanisms in each of the Member States should be a priority for their respective defence policies.

The use of cyber means in peacetime – with actors operating below the threshold of armed conflict and to advance their strategic interests – and wartime raises serious challenges for public and private actors regarding the rules and regulations applicable to cyberattacks, and the cooperation between and among stakeholders. The **EU Cyber Solidarity Act (CSA)** proposed by the European Commission takes into account the commitment set in the Joint Cyber Defence Communication and aims to boost cross-border and public-private coordination in anticipating and tackling cyberattacks as part of a broader cybersecurity package. Private companies stand on the forefront of cyber resilience and must be actively involved in cyber response. The call for closer cooperation between public and private entities echoes a model already in place in Ukraine, where companies and authorities successfully collaborate to deal with cyber threats. The Estonian Defence League's Cyber Unit provides another formative example. As early as the year 2000, cooperation among information security specialists started in Estonia. The Cyber Unit's mission includes the protection of information infrastructure and supporting broader objectives of national defence[53].

The CSA includes a European Cybersecurity Shield composed of Security Operations Centres (SOCs) and a comprehensive Cyber Emergency Mechanism, to create a better cyber defence method. The Cyber Shield will be tasked with improving detection, analysis and response to cyber threats, using advanced AI and data analytics to detect and share warnings on such threats with authorities across borders. Beyond sectors, the interconnections of operational SOCs in the EU under the EU Cybersecurity Shield should ensure 24/7 response, exchange of tools, talents, processes, and allow for secondment of talents for national reserve pools such as cybersecurity reserve, civil service, military service, and others. Member States should also make better use of EUROPOL to exchange intelligence about cross border cybercrime, including technical information on cyberattacks coming from the EU network of CERTs.

Several lessons from the cyber dimension of the war in Ukraine are being addressed under the CSA. Firstly, given the spill-over effect of cyberattacks and the need to defend against them in cooperation, sharing information among countries under an agreed framework and further mainstreaming EU cyber crisis management and rapid response is vital for the EU's resilience and defence. Secondly, lessons learned show the wide use and deployment of AI tools in Ukraine's cyber defence. This area will increase in importance, as the use of large language models and generative AI can provide a strategic advantage in both carrying out and preventing cyberattacks.

The **Directive on measures for a high common level of cybersecurity across the Union (NIS2)**[54] is a step to improve the resilience and incident response capacities of both the public and private sectors in the EU. The Directive introduces key requirements for essential[55] and important service providers in critical sectors, including reporting cyberattacks, implementing security policies, scrutinising the security of

[52] European Council,'Council Conclusions on the EU Policy on Cyber Defence', 23 May 2023, Available at: https://www.consilium.europa.eu/media/64526/st09618-en23.pdf.

[53] More information about the Estonian Defence League's Cyber Unit (EDL CU) is available at: https://www.kaitseliit.ee/en/cyber-unit.

[54] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

[55] The Directive classifies services into two categories, essential entities and important entities, reflecting the extent to which they are critical as regards their sector or the type of service they provide, as well as their size. The Directive does not apply to entities carrying out activities in areas such as defence or national security. Maturity level in the field of cyber defence varies across Member States and there is no holistic approach for cyber defence of the bloc.

suppliers, and the use of encryption technology. Building the capacities of entities to implement the new requirements will be vital, as they have different levels of readiness and agility to adopt the obligation. Industry and governments alike are struggling with stretched cyber resources, and it is important to ensure a practical approach to deliver results. Therefore, the European Commission and ENISA should closely cooperate with the Member States and coordinate sector-based cyber preparedness exercises. This initiative is an opportunity for building more evidence-driven understandings into the scope and impact that cyberattacks present to critical civilian infrastructure sectors, and the potential harm and impact on the people. The NIS2 Directive can be also used as the framework to map the sectors at risk. ENISA can play a role in accelerating EU wide recommendations and lessons learned across sectors.

The NIS2 Directive serves as an example for candidate countries that seek to align their legislation with the EU acquis and can help the aspirant countries to increase their cyber posture. This step is particularly important as they are more vulnerable to a potential cyber aggression considering their geopolitical context. However, given the compliance period for transposition of the NIS2 Directive[56], the effects will not be reflected in improved cyber posture immediately. Since posture, threat landscape and cyber ecosystem are changing rapidly, it would be recommended to elaborate a mechanism for speedy implementation of holistic EU-wide policies for cyber defence and resilience.

As cyber operations are taking a hybrid form with an observed nexus between cyberattacks and the manipulation of the information ecosystem, the European Commission should ensure that national implementation of the NIS2 Directive, the European Regulation on Terrorist Content Online (TCO), and the Digital Services Act (DSA) is coordinated, using interoperable standard and processes, and do not hamper coordination when a crisis hits.

The Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware has laid the groundwork for stricter rules on surveillance technologies. Based on the Committee's findings and recommendations, the report adopted by the European Parliament on 15 June 2023[57] outlines the reforms necessary to curb spyware abuse. In line with the need to restore and strengthen the institutional and legal safeguards on the use of spyware by governments, the Member States should also stop financing unethical vulnerability research and procuring targeted surveillance solutions, as this creates a disproportionate risk to the cybersecurity of the bloc.

While critical infrastructure providers are subject to strict rules stemming from NIS and NIS2, providers of hardware and software have not been fully covered by the current EU policy and regulatory framework. The **Cyber Resilience Act (CRA)** aims to close the gaps that create vulnerabilities in the cyber ecosystem by establishing cybersecurity requirements before and after a product is marketed, to strengthen the security and resilience of the supply chain. The proposal aims to support the detection and awareness of cybersecurity threats and incidents, bolster the preparedness of critical entities, as well as reinforce solidarity, concerted crisis management, and response capabilities across the Member States. To reach its objectives, it should follow a risk-based approach to keep the framework proportionate and manageable for a wide range of entities in the supply chain, since not all devices/software bear the same risk. Important lessons can be learned from the war in Ukraine and the cyber preparedness of the country's infrastructure, which has adopted horizontal approaches to cybersecurity. Cross-ecosystem consistency and coherence

[56] The NIS2 was adopted on 16 January 2023 with a 2-year period during which Member States must implement the measures stipulated in the Directive into their national legislation.
[57] European Parliament, 'Spyware: MEPs call for full investigations and safeguards to prevent abuse', Press Release, 15 June 2023, Available at: https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse.

are crucial to avoid fragmentation of the EU's cyber ecosystem, and strengthen the cybersecurity of interconnected ICT products, services, and components.

Vulnerability disclosure is an important part of both the proposed CRA and the adopted NIS2 Directive. With the NIS2 Directive, Member States will need to have a coordinated vulnerability disclosure policy[58]. In addition, vulnerability handling requirements are also foreseen in the CRA. In line with these provisions, the European Commission should promote the protection of vulnerability disclosure, and EU Member States should enforce Coordinated Vulnerability Disclosure (CVD) mechanisms, including accelerating amendments to criminal laws to protect security researchers, and ENISA to operationalize the usage of the EU Vulnerability database (EUVDB).

The EU is also the most advanced in terms of implementing AI policy and legislation, with the **Artificial Intelligence Act (AI Act)** aiming to ensure that AI systems within the EU are safe and consistent with current laws and principles, as well as to address dangers, ethical problems, and other challenges related to the use of AI systems. According to threat landscapes, there is evidence that the first generation of AI-enabled cyberattacks have been utilised[59]. This has also been seen in the context of the Ukrainian conflict, with the employment of cyber methods for disinformation operations, such as the hacking of media outlets and the circulation of deep fake videos. It is critical that the risks connected with the harmful use of developing technologies is appropriately recognised within the scope of this regulation. In that regard an accountability framework should be clear and reinforced. It is also critical that this regulation safeguards potential victims, and that particular steps are implemented, such as detecting and preventing malicious use, as well as providing clear guidelines and channels for those who have been negatively impacted by AI to seek redress and reparation.

The EU initiatives necessitate broad stakeholder inclusion to exchange best practices and deepen understanding of the cyber landscape. An evidence-based approach will help to ensure that cybersecurity regulations address actual needs and help overall cybersecurity preparedness by reducing the risk of cyberattacks. It will also help to keep stakeholders on the same level of adherence to standards. A skilled cybersecurity workforce can support the ability of companies to comply with high standards that will be included in the proposed cybersecurity regulation, and increased readiness for essential parts of critical information infrastructure. In this regard, the **Cybersecurity Skills Academy**[60] that was recently launched by the European Commission is a positive step forward as a multi-stakeholder initiative aiming to close the cybersecurity sector's ongoing skills shortage and develop the EU's cyber resilience.

The European Commission should financially support independent civil society organisations to support EU efforts in a range of cyber resilience and defence activities. The non-exhaustive list includes building a pool of cyber volunteers to join the EU Cybersecurity Reserve; detecting cyber operations against EU civilians, civilian objects and critical infrastructure; facilitating reporting of attacks by vulnerable communities, and helping them access support from national CERTs and law enforcement agencies; in coordination with the EU Cybersecurity Incident Review Mechanism, mapping and measuring the human cost and societal impact of cyberattacks, notably to inform about the human impact of crowdsourcing of cyberattacks; forecasting how the convergence of disruptive tech (for example generative AI and large language models) and disruptive regulations (including the AI Act and CRA) will impact the EU security

[58] Member States will need to have a coordinated vulnerability disclosure policy adopted and published by 17 October 2024. More information: https://www.enisa.europa.eu/news/coordinated-vulnerability-disclosure-towards-a-common-eu-approach.

[59] European Union Agency for Cybersecurity (ENISA), 'ENISA Threat Landscape 2022', 3 November 2022. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[60] Digital Skills & Jobs Platform, 'Cybersecurity Skills Academy: a coordinated approach to boost the EU cyber workforce', Available at: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy.

architecture; independently supporting the evaluation of how the private sector is properly implementing EU regulations (TCO, DSA, NIS2, CRA, AI ACT).

Multidimensional warfare is a complex security challenge. Responding to its new realities necessitates leveraging and harmonising interconnected EU initiatives, and balancing preventive measures and cyber resilience with instruments that can respond to cyberattacks when they happen. Both resilience initiatives and defence and diplomatic strategies must consider the coordination of multiple threats, and leveraging policy responsiveness and technical innovation. Capacity building plays a key role in ensuring that policies are operationalised and also informed by lived realities. The capacity building and funding streams must be matched across the board in order to support the EU and Member Countries in their efforts to build cyber resilience. While cyber policies in the EU have matured significantly over the past ten years – and cyber has become a priority area – the funding lags behind, and this imbalance needs to be corrected.

The EU implemented several legal and strategic initiatives to strengthen Member States' resilience against cyber threats, including **reinforced cooperation with NATO** in the field of cyberspace prior to the war in Ukraine[61]. NATO and the EU are cooperating through a Technical Arrangement on Cyber Defence, which was signed in February 2016. Since the start of the war, NATO and the EU have explored further areas of engagement on cyber defence that would complement the EU's capabilities in cyber resilience. While NATO leads on cyber defence, it does not impose sanctions. EU-NATO cooperation is therefore key to providing complementary value to each other. This cooperation can also contribute to improved attribution based on technical evidence, which is a key part of increased accountability in cyberspace. With the rising impact of cyberattacks – both in terms of the severity of damage and number of victims – the challenge of accountability needs to be prioritised by decision-makers at all levels.

More needs to be done towards accountability on all levels – and attribution on technical, legal, and political levels – to ensure that existing laws and norms are respected. This will advance the goal of protecting people and allowing them to seek redress if they fall victim to a cyberattack. Responses and measures targeted at individuals, groups, or governments need to be respectful of international law, and tailored to hold the aggressors accountable and discourage misconduct. In this light, the EU sanctions regime, evolved from the **Cyber Diplomacy Toolbox,** represents a set of measures for accountability in cyberspace. While the toolbox is a successful EU instrument, it has shown some limitations responding to the war in Ukraine. The multidimensional crisis has shown that the toolbox needs to be further mainstreamed into the wider EU structure to reflect on the real-life integration of cyber into other domains. An important part of the toolbox is an option to impose sanctions. However, economic sanctions have only been implemented via the Ukrainian territorial regime in select cases. This was possible because these sanctions are connected to cyberattacks deployed against Ukraine. The EU does not have a regime which would allow economic sanctions if an attack was conducted against Member States, and this is a gap that will need to be addressed together with sectoral sanctions (for example, export controls on dual-use technology).

The Cyber Diplomacy Toolbox would further benefit from broader situational awareness that addresses the need for foreign policy perspectives. Cooperation with private companies, especially in information exchange, has been ongoing within the framework of ENISA and Europol, but multi-stakeholder efforts can further complement states' analytical capacity regarding data on how the threat landscape is evolving, how to interpret the data within specific contexts, and how to increase understanding of the impact of cyberattacks. Many stakeholders, including civil society organisations and academia, have expertise and experience based on proximity to victims, which helps build a body of knowledge about the impact and

[61] NATO and the EU are cooperating through a Technical Arrangement on Cyber Defence, which was signed in February 2016. On 14 July 2022, senior officials from NATO and the EU met to take stock of recent developments in the cyber threat landscape and explore further areas of engagement on cyber defence.

harm to civilians stemming from cyberattacks and operations. The EU should tap into this potential, and allocate funding to support independent tracing of cyber threats in conflict situations and their impact.

Beyond diplomatic measures, governments have a duty to protect individuals, thus not only assuming the political costs of publicly attributing a cyberattack, but also employing all the available means to hold the actors responsible accountable. The EU should use this opportunity to further progress implementation of the framework of responsible state behaviour in cyberspace as a key step towards accountability, including addressing the challenges that the unique characteristics of cyber raise for the interpretation and application of international law. Member States should increase efforts toward common interpretation of international law in cyberspace. While interpretation of international law in the area of international security is the competence of Member States, the EU could outline an ambition to arrive at common positions.

II. Workshop proceedings

WORKSHOP PROCEEDINGS

The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict

Table of contents

1 Programme

For the Subcommittee on Security and Defence (SEDE)

WORKSHOP
The role of cyber in the Russian war against Ukraine: its impact and the consequences for the future of armed conflict

Thursday 29 June 2023

09:30 - 11:00

Brussels, Altiero Spinelli building, room A1E-2

PROGRAMME

09.30-09.35 **Welcome and introductory remarks**

- ***Nathalie Loiseau***, MEP, Chair of the Subcommittee on Security and Defence

09.35-10.05 **Presentation of the briefing paper '*The role of cyber in the Russian war against Ukraine: its impact and the consequences for the future of armed conflict*'**

- ***Stéphane Duguin***, Chief Executive Officer, CyberPeace Institute, Geneva
- ***Pavlina Pavlova***, Public Policy Advisor, CyberPeace Institute, Geneva

10.05-10.55 **Debate with Members**

10.55-11.00 **Concluding remarks**

- ***Nathalie Loiseau***, MEP, Chair of the Subcommittee on Security and Defence

2 Welcome remarks: Nathalie Loiseau, MEP, Chair of the Subcommittee on Security and Defence

Dear colleagues,

We begin our session today with a workshop on the role of cyber in the Russian war against Ukraine, its impact and consequences for the future of armed conflicts. I welcome our panellists, Mr. Stéphane Duguin, Executive Director of the NGO CyberPeace Institute in Geneva and Mrs. Pavlina Pavlova, Public Policy Advisor at the CyberPeace Institute.

On February 24, 2022, Russia launched a general offensive - land, air and sea - accompanied by cyberattacks aimed at destroying strategic data, paralyzing critical infrastructure, inflicting maximum civilian and military damage and destabilizing the civilian population.

Experts do not all agree on the scale and impact of Russian cyberattacks. What is clear is that they have increased massively, even if they had been going on for years, against Ukraine's infrastructure and many public institutions, but also against countries that support Ukraine.

Cyber warfare is increasingly being waged outside the military or governmental sphere. Ukraine is no exception to this reality. An estimated 270,000 volunteers are self-coordinating, deciding, planning and executing strikes on Russian cyber infrastructure, without direct government supervision. These cyber activists have been around since the 1990s, but today they are more like an “auxiliary cyber force,” playing a supporting role in a broader military effort.

In cyberspace, the difficulty of distinguishing between official attacks perpetrated by States and those of cyber-activists raises the problem of the attribution of attacks and the status of these cyber-activists. When states carry out attacks on critical infrastructure by hiding behind criminal organizations acting as intermediaries, it is difficult to prove the links between states and these organizations, even though last weekend gave us some information on the role of mercenaries as merely another form of warfare that a state can wage.

This war has also highlighted the importance of cyberspace for the EU, which has become aware of its strategic dimension with respect to the dependence on digital technologies. There is progress to be made to reduce the disruption caused by a growing number of cyberattacks, and the EU must make progress in countering the malicious actions of authoritarian regimes across the spectrum of hybrid warfare.

Mr. Duguin and Mrs. Pavlova will present their analysis of the cyber dimension of the war in Ukraine. How does cyber fit into conventional high-violence warfare, and what can you tell us about Ukraine's strengths and weaknesses in the face of Russian cyberattacks? What lessons can already be learned from the war in Ukraine, in terms of resilience, but also in terms of counter-offensive? What recommendations can you offer to make us better deal with these threats? And with these first questions, I give you the floor.

3 PowerPoint presentation: The role of cyber in the Russian war against Ukraine: its impact and the consequences for the future of armed conflict

ECORYS
CyberPeace Institute
FINANC
Putin's forces

The role of cyber in the Russian war against Ukraine:

Its impact and the consequences for the future of armed conflict

Stéphane Duguin, Chief Executive Officer

Pavlina Pavlova, Public Policy Advisor

CyberPeace Institute

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY //** [illegible]

CyberPeace Institute
CYBERPEACEINSTITUTE.ORG

Cyber dimension of the war in Ukraine

The **CyberPeace Institute** has been documenting cyberattacks on critical infrastructure and civilian objects since the beginning of the Russian war of aggression against Ukraine.

As of 1 June 2023:

1 998 cyberattacks and operations

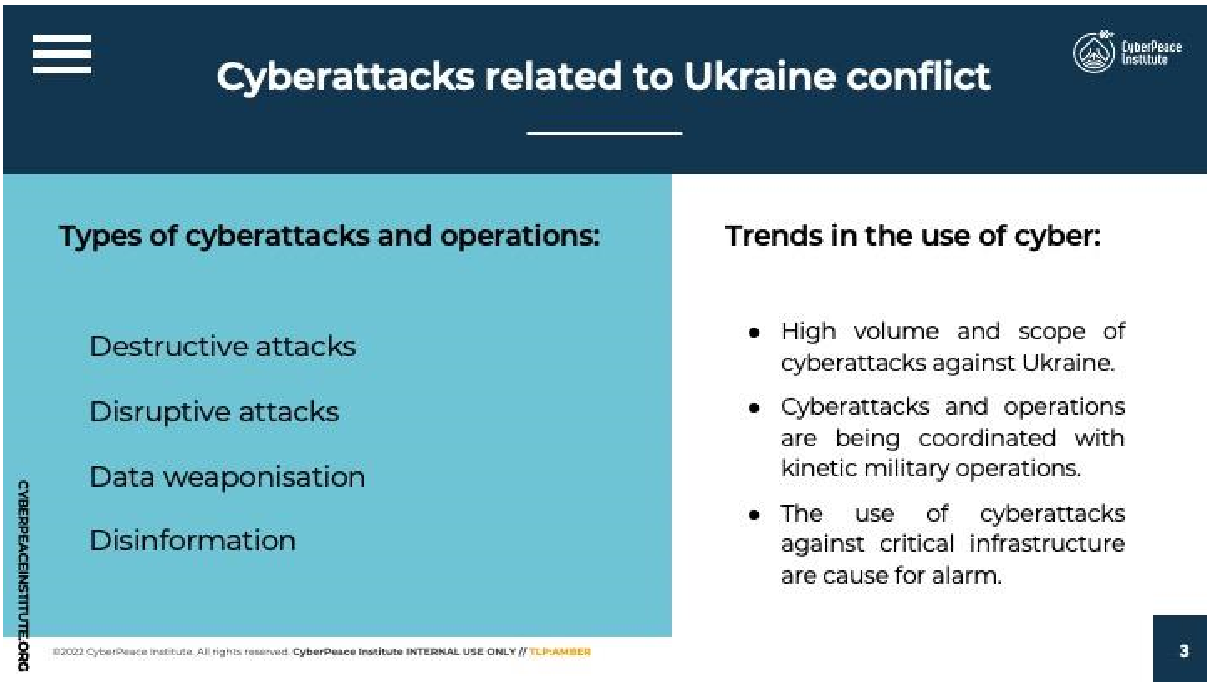
100 different actors targeting

23 critical infrastructure sectors

51 countries

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY // TLP:AMBER**

2



CyberPeace Institute

Cyberattacks related to Ukraine conflict

Types of cyberattacks and operations:

Destructive attacks

Disruptive attacks

Data weaponisation

Disinformation

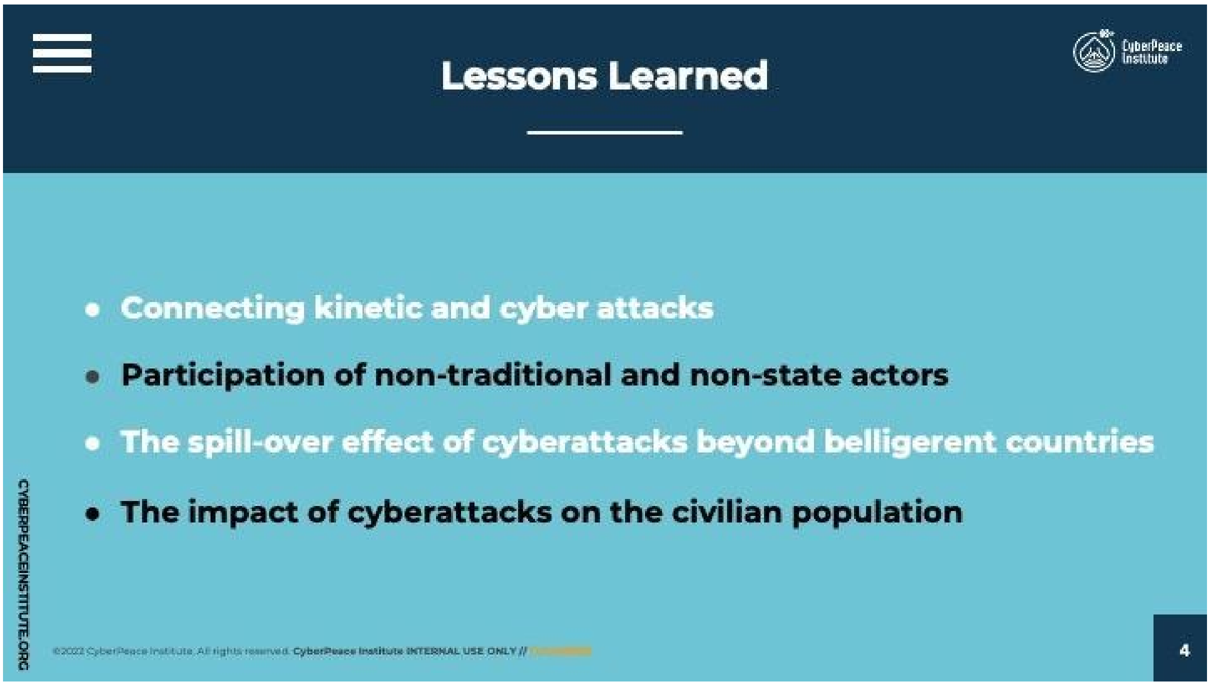
Trends in the use of cyber:

- High volume and scope of cyberattacks against Ukraine.
- Cyberattacks and operations are being coordinated with kinetic military operations.
- The use of cyberattacks against critical infrastructure are cause for alarm.

CYBERPEACEINSTITUTE.ORG

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY** // TLP:AMBER

3



CyberPeace Institute

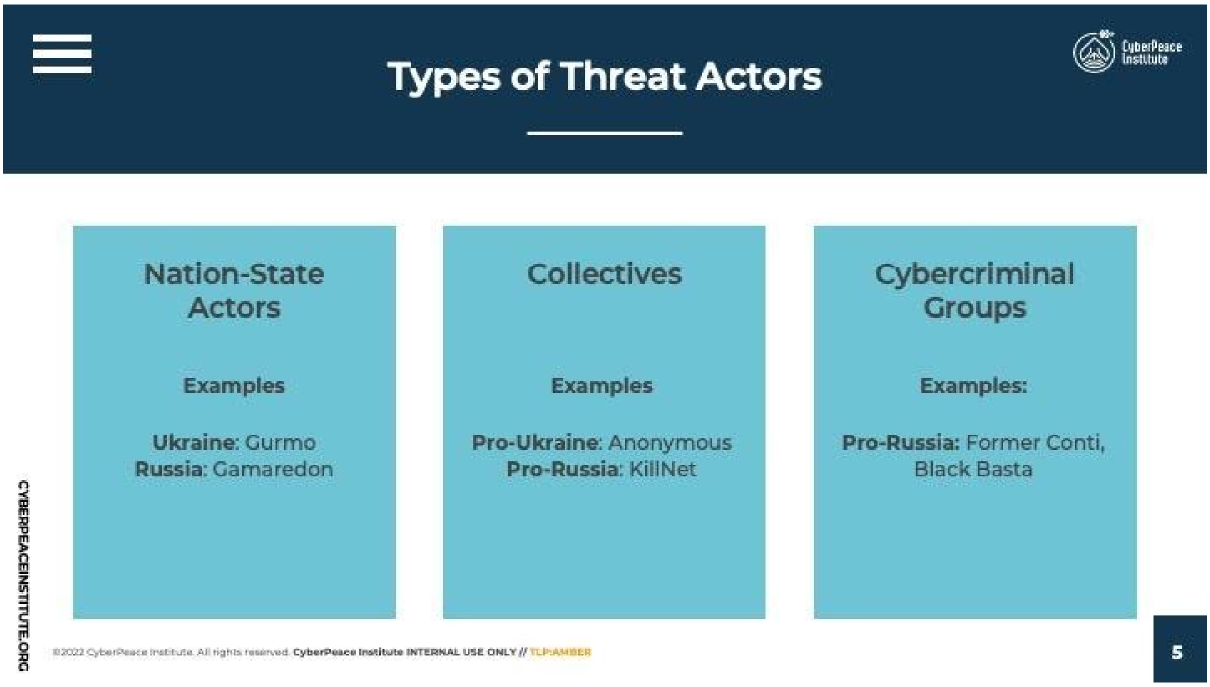
Lessons Learned

- **Connecting kinetic and cyber attacks**
- **Participation of non-traditional and non-state actors**
- **The spill-over effect of cyberattacks beyond belligerent countries**
- **The impact of cyberattacks on the civilian population**

CYBERPEACEINSTITUTE.ORG

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY** //

4



Types of Threat Actors

Nation-State Actors

Examples

Ukraine: Gurmo
Russia: Gamaredon

Collectives

Examples

Pro-Ukraine: Anonymous
Pro-Russia: KillNet

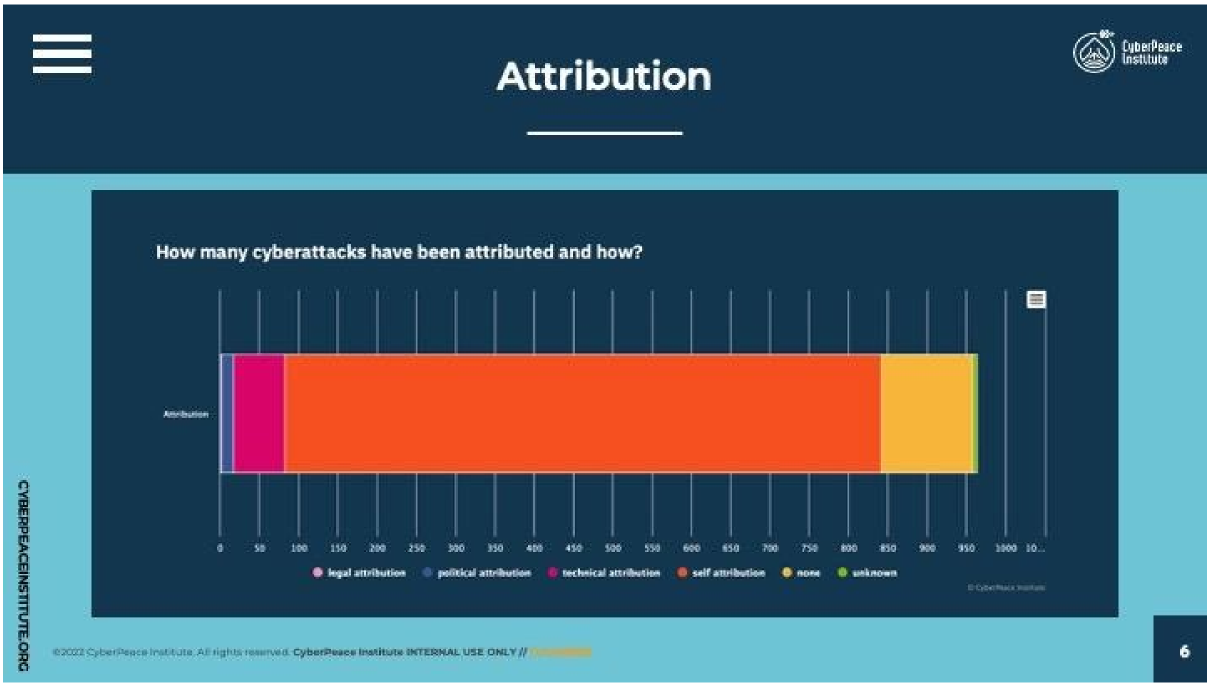
Cybercriminal Groups

Examples:

Pro-Russia: Former Conti, Black Basta

CYBERPEACEINSTITUTE.ORG

5

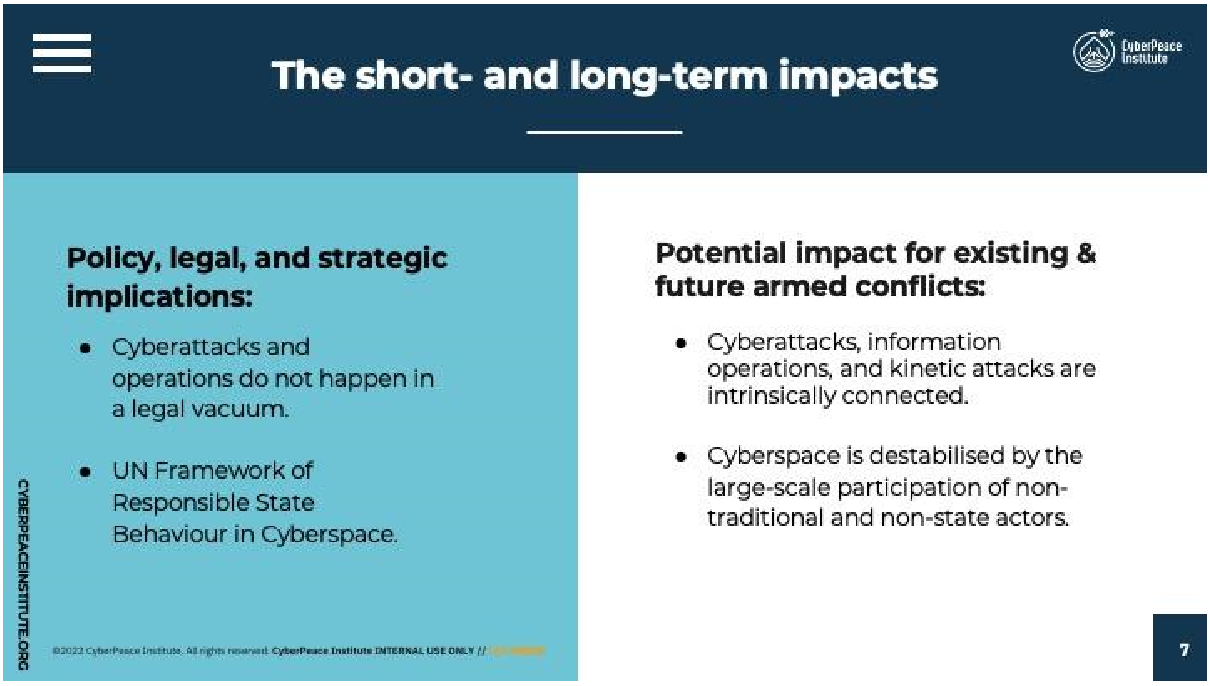


Attribution

How many cyberattacks have been attributed and how?

CYBERPEACEINSTITUTE.ORG

6



The short- and long-term impacts

CyberPeace Institute

Policy, legal, and strategic implications:

- Cyberattacks and operations do not happen in a legal vacuum.
- UN Framework of Responsible State Behaviour in Cyberspace.

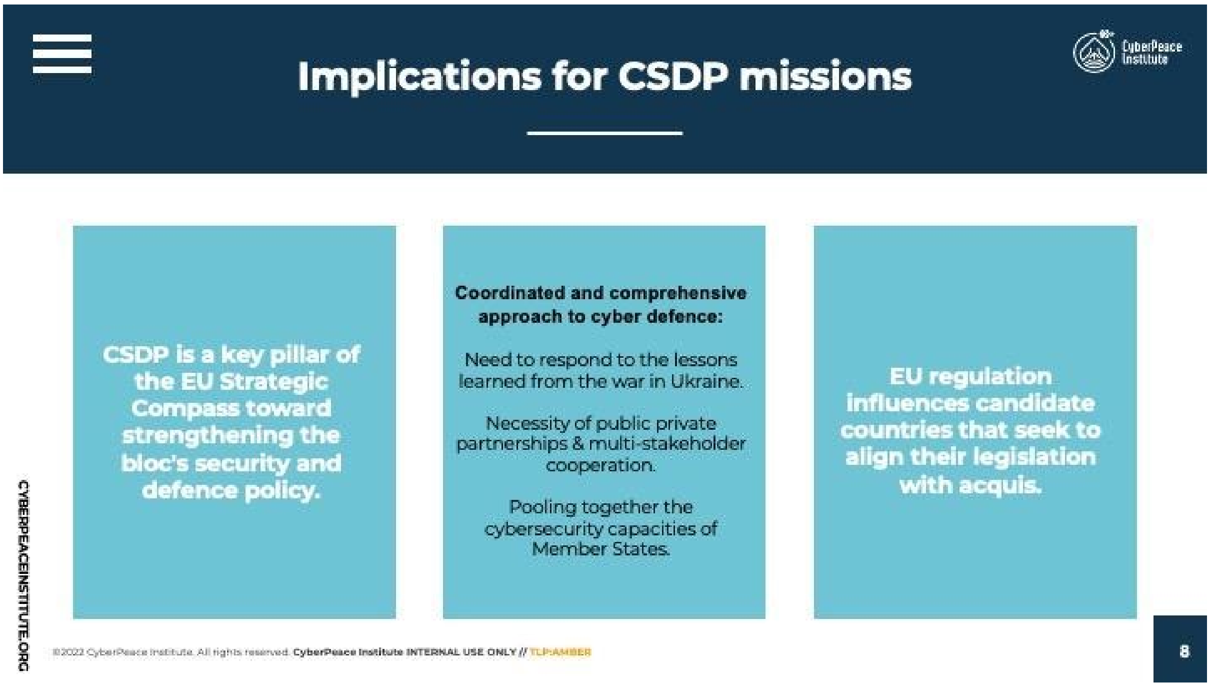
Potential impact for existing & future armed conflicts:

- Cyberattacks, information operations, and kinetic attacks are intrinsically connected.
- Cyberspace is destabilised by the large-scale participation of non-traditional and non-state actors.

CYBERPEACEINSTITUTE.ORG

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY // TLP:AMBER**

7



Implications for CSDP missions

CyberPeace Institute

CSDP is a key pillar of the EU Strategic Compass toward strengthening the bloc's security and defence policy.

Coordinated and comprehensive approach to cyber defence:

Need to respond to the lessons learned from the war in Ukraine.

Necessity of public private partnerships & multi-stakeholder cooperation.

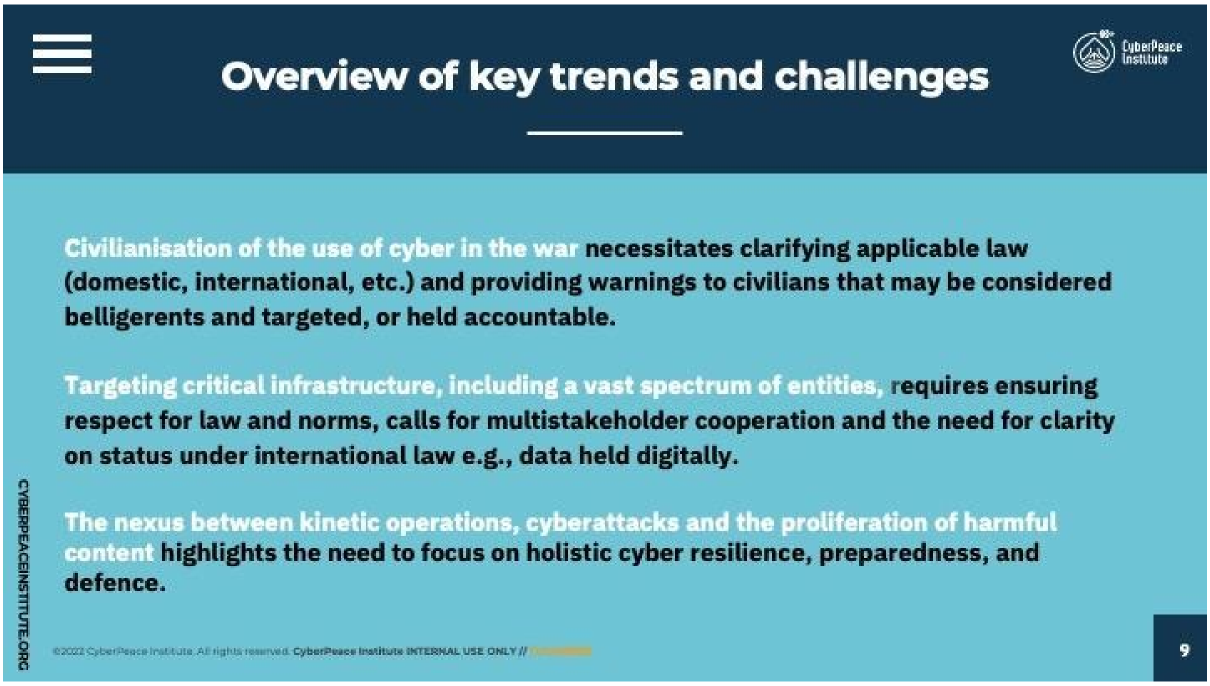
Pooling together the cybersecurity capacities of Member States.

EU regulation influences candidate countries that seek to align their legislation with acquis.

CYBERPEACEINSTITUTE.ORG

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY // TLP:AMBER**

8



Overview of key trends and challenges

CyberPeace Institute

Civilianisation of the use of cyber in the war necessitates clarifying applicable law (domestic, international, etc.) and providing warnings to civilians that may be considered belligerents and targeted, or held accountable.

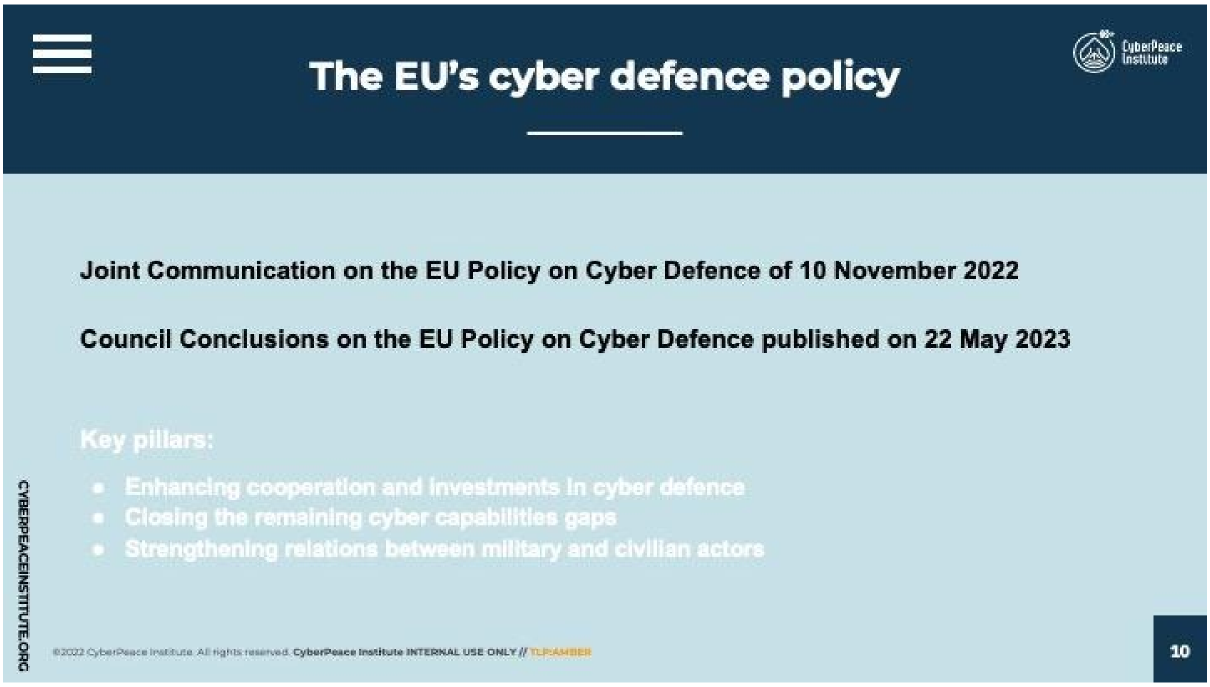
Targeting critical infrastructure, including a vast spectrum of entities, requires ensuring respect for law and norms, calls for multistakeholder cooperation and the need for clarity on status under international law e.g., data held digitally.

The nexus between kinetic operations, cyberattacks and the proliferation of harmful content highlights the need to focus on holistic cyber resilience, preparedness, and defence.

CYBERPEACEINSTITUTE.ORG

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY //** [illegible]

9



The EU's cyber defence policy

CyberPeace Institute

Joint Communication on the EU Policy on Cyber Defence of 10 November 2022

Council Conclusions on the EU Policy on Cyber Defence published on 22 May 2023

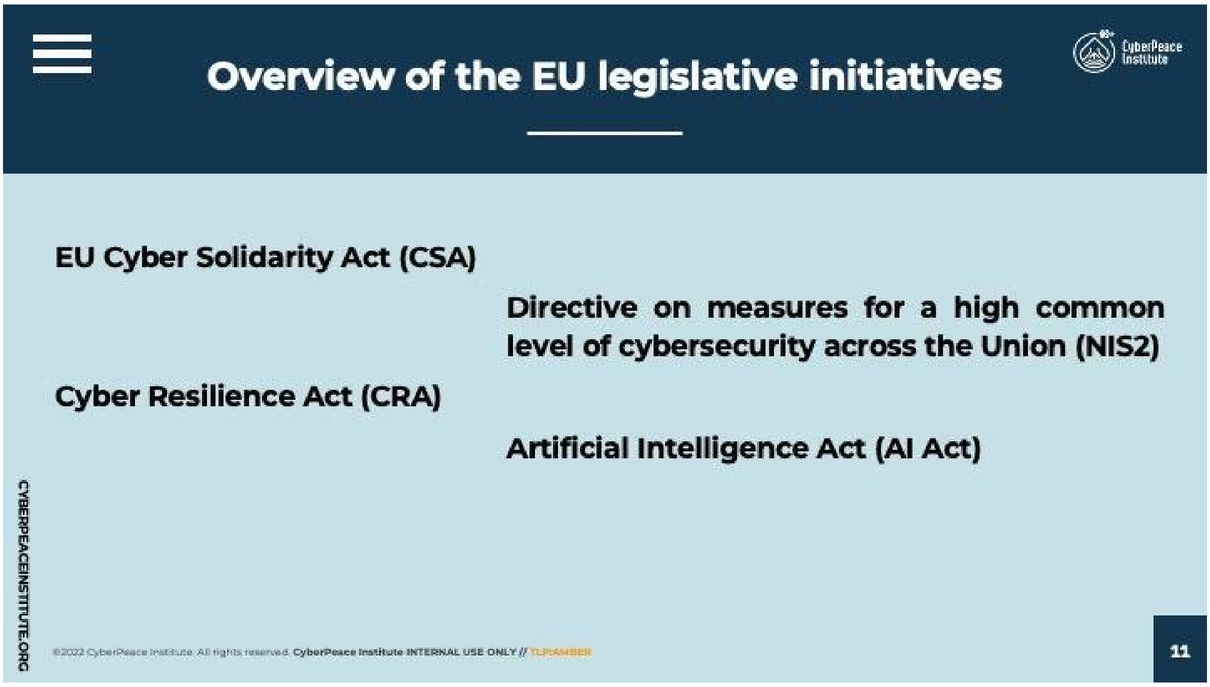
Key pillars:

- **Enhancing cooperation and investments in cyber defence**
- **Closing the remaining cyber capabilities gaps**
- **Strengthening relations between military and civilian actors**

CYBERPEACEINSTITUTE.ORG

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY //** TLP:AMBER

10



Overview of the EU legislative initiatives

EU Cyber Solidarity Act (CSA)

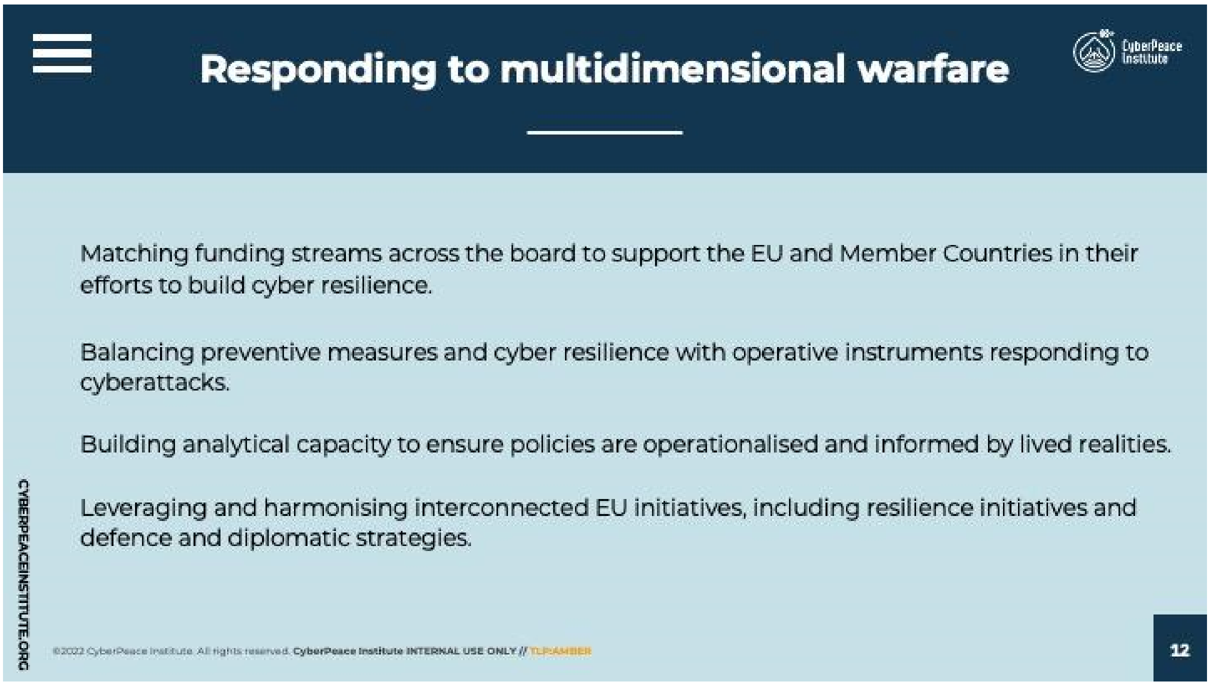
Directive on measures for a high common level of cybersecurity across the Union (NIS2)

Cyber Resilience Act (CRA)

Artificial Intelligence Act (AI Act)

CYBERPEACEINSTITUTE.ORG

11



Responding to multidimensional warfare

Matching funding streams across the board to support the EU and Member Countries in their efforts to build cyber resilience.

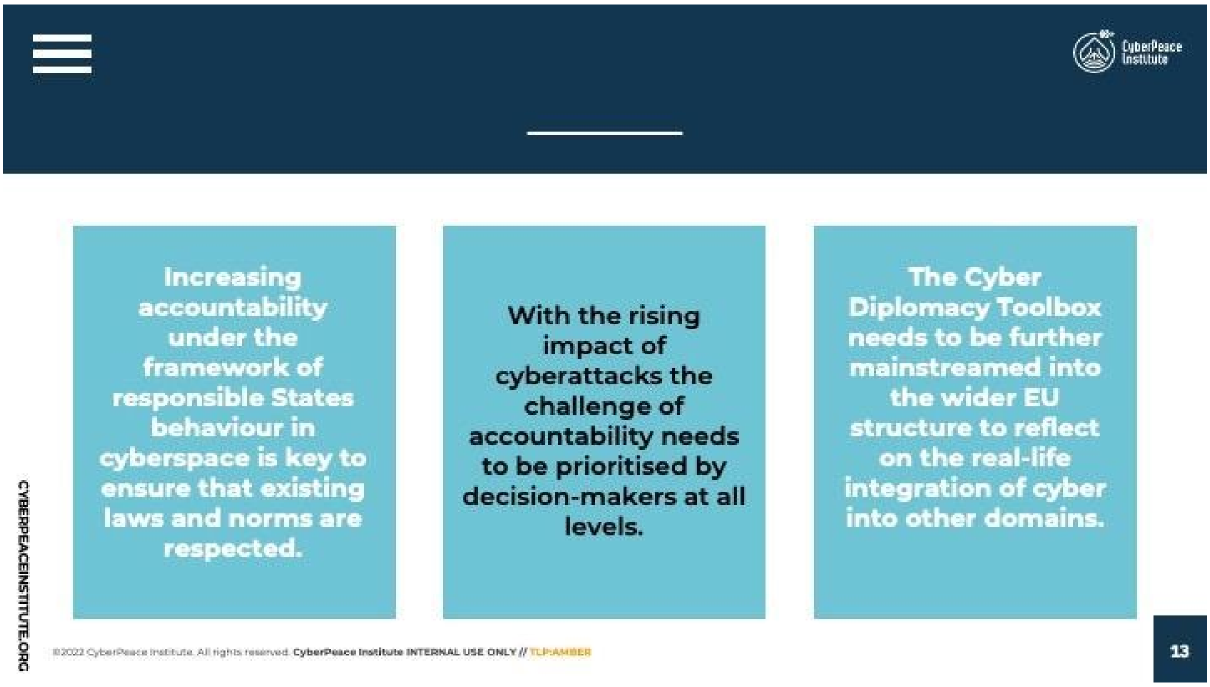
Balancing preventive measures and cyber resilience with operative instruments responding to cyberattacks.

Building analytical capacity to ensure policies are operationalised and informed by lived realities.

Leveraging and harmonising interconnected EU initiatives, including resilience initiatives and defence and diplomatic strategies.

CYBERPEACEINSTITUTE.ORG

12



Increasing accountability under the framework of responsible States behaviour in cyberspace is key to ensure that existing laws and norms are respected.

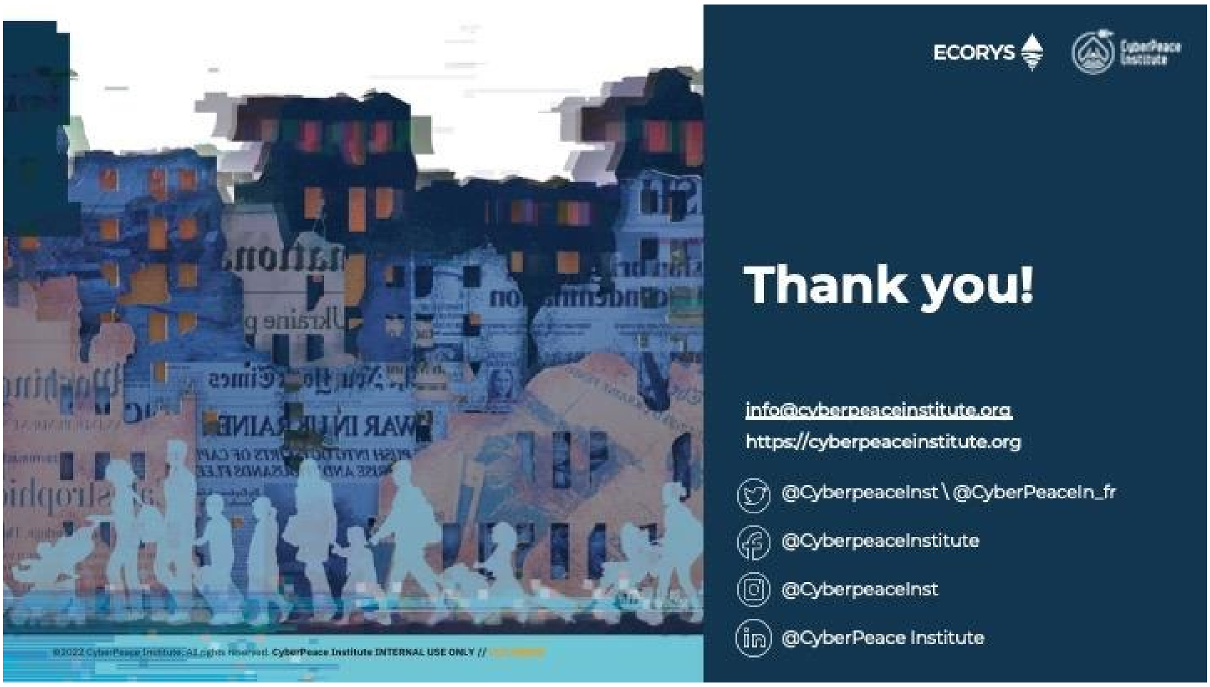
With the rising impact of cyberattacks the challenge of accountability needs to be prioritised by decision-makers at all levels.

The Cyber Diplomacy Toolbox needs to be further mainstreamed into the wider EU structure to reflect on the real-life integration of cyber into other domains.

CYBERPEACEINSTITUTE.ORG

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY // TLP:AMBER**

13



Thank you!

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

@CyberpeaceInst \ @CyberPeaceIn_fr

@CyberpeaceInstitute

@CyberpeaceInst

@CyberPeace Institute

©2022 CyberPeace Institute. All rights reserved. **CyberPeace Institute INTERNAL USE ONLY //** [illegible]

4 Debate with Members

Raphaël Glucksmann, MEP, Chair of the Special Committee on foreign interference in all democratic processes in the European Union, including disinformation, and the strengthening of integrity, transparency and accountability in the European Parliament and Member of the Subcommittee on Security and Defence, highlighted that the Special Committee he chairs recently visited Kyiv and was impressed by the efforts that Ukraine was making in terms of cyber resilience, working with Western organizations, including NATO. The experts mentioned accountability and the Special Committee is very active in this regard. MEP Glucksmann asked the experts to expand on the consequences for criminal organizations that are attacking infrastructure in Ukraine, but also in Europe in general. Have there been any changes or trends noticed in the type of consequences for these actors, as it seems not much has been done? In terms of modus operandi – various procedures have been observed so far. Has the trend of decentralization been observed in regard to Russia and China? Are Chinese and Russian actors who are conducting cyberattacks linked to the security services of these countries? In China, for example, have you noticed any cooperation between the Russian and Chinese actors in cyber warfare? Additionally, concerning the help that the EU countries can offer to Ukraine on cyber defence – are there any gaps or shortcomings in this regard? And what can be said about European private actors? Are there private actors in Europe that contribute to Ukraine's cyber defence? Finally, what is the assessment of how seriously private actors are being taken in Europe in regard to cyber defence? Because, if you look at the investments in technology – the comparison between the US and the EU investments is stark.

Sven Mikser, MEP, Vice-Chair of the Delegation for relations with the NATO Parliamentary Assembly and Member of the Subcommittee on Security and Defence, stressed that when the Russian aggression started in February last year, before the invasion, there have been many speculations about how advanced the Russian conventional military modernization and re-armament had been. When the fighting had been going on for some time, it became clear that much of that assessment had been hyped and that many of the systems did not make it into mass production and nothing had been delivered to the troops and Russia has been relying on old legacy systems. What surprised us the most was not what was new but the fact that Russia did it very much the old way. When it comes to cyber, what has this war revealed regarding Russian capabilities? Was there anything pragmatically new, something that we did not expect them to do or was that quite what we were prepared for? Secondly, cyberattacks have become and will continue to be an integral part of any kinetic military operation and they are becoming more sophisticated technically. They are very disruptive and can potentially be even more disruptive. However, generally, in the expectations of the military conflict, regarding the lethality of cyber operations, these assessments have been scaled down somewhat recently. Can the experts share an example of when cyber operations had a strategic impact on the course of the war?

Andrius Kubilius, MEP, Chair of the Delegation to the Euronest Parliamentary Assembly and Member of the Subcommittee on Security and Defence, underscored that the presentation focused on responsibility, which is key, but in times of war in Ukraine, we are speaking about the international tribunal for war crimes which moves very slowly. How can we implement more accountability for cyberattacks? Secondly, regarding technology, in this war, we understood a lot about traditional military and technology, and we understand what Ukrainians need. The question in terms of cyber warfare is what is really needed to defend a country against such attacks. Can the experts elaborate on what we should look for?

Bart Groothuis, MEP, Vice-Chair of the Delegation for relations with Iran and Member of the Subcommittee on Security and Defence, expressed that he found it remarkable that the presentation mentioned the nexus between criminal actors as an instrument of the foreign policy of Russia – criminal actors being used by the Russian state. He urged to look at the Wagner Mercenary Group, and its Founder, Yevgeny Prigozhin, who is also the Chief of the Internet Research Agency. What can be said about any cyber gangs, not including disinformation, related to the Wagner Group? Secondly, in regard to disinformation, MEP Groothuis proposed some amendments in the Digital Services Act that oblige platforms to put watermarks any time there is synthetic media on the platform to make people aware of this. This amendment was included in the Parliament's position, but big tech lobbyists managed to remove it from the trialogue, and it is not part of the Digital Services Act. What else can the EU do to watermark this content to ensure that any synthetic media put online are watermarked and labeled? Finally, the nexus between kinetic operations and cyberattacks is also present in the possible sabotage of subsea internet cables. Last week, the port of Olenya in Russia which harbors the GUGI Institute that is closely related to Russia's intelligence – possibly the instrument that Russia can use to sabotage these cables – had its defenses hardened. What can be the reasons behind these actions? And how can we address such threats?

Stéphane Duguin, Chief Executive Officer, CyberPeace Institute, began by answering the question about the consequences for criminal organizations. It is important to remember that what countries did not achieve during peacetime will be very difficult to accomplish in wartime. For decades now, States have been struggling to effectively investigate and prosecute cybercrime – it is not impossible, there is rather a myth that it is not possible to investigate cybercrime. Work has been done in this context against cyberterrorism and cybercrime, but there is a further need for international cooperation. Cybercrime is essentially interconnected. Member States need to work together to build response and push for accountability. Coordination between the diverse actors in cyberspace is essential. This also includes physical infrastructure, such as cables and other networks, that are not owned by Member States. In cyberspace, one must think about who controls the infrastructure. Those who control the infrastructure control the information. In terms of response, if countries do not consider all the aspects, the networks, the generation of content, and legal international cooperation, governments will not manage to tackle the problems. Indeed, there is a genuine will to address these issues – there are proposals for new rules in the area of cybersecurity and online content – but these initiatives need to be coordinated. Otherwise, the EU will have different offices working on overlapping issues. Today, we were talking about the decentralization of cyberspace, and this is linked to the issue of accountability. The experts can have theories about why more than a hundred actors have been involved in committing cyberattacks since the invasion of Ukraine. Are they different actors or not? It can be a useful ploy – one actor can be pretending to be ten or twenty actors because that makes it look like there were more people involved in the war. If there is a targeted cyberattack, but it is split up between individual actors there is a higher chance of falling below the radar in terms of facing prosecution. The Institute does not have the data yet to verify this theory, but we want to identify the reality behind all these actors and actions. Still, there is a persistent lack of information and data to prove the link between coordinated and centralized actors pretending to be decentralized. At the same time, there is a general phenomenon of decentralization that is not new – crowdsourcing is part of the internet culture and this is a societal problem. It is worrying that anyone anywhere on this planet can get up in the morning and decide whether they will attack a military base in Russia with something that can be activated in a few seconds. This is posing the question about ethical behaviour on the internet that goes beyond the question of war and becomes a societal problem. There was a question about a specific cyberattack of strategic importance with a focus on Russian capabilities against Ukraine. These cyberattacks began before the war. There were ten years when these attacks had been going on – such as the NotPetya attack, but there were many others that showed that there were attempts to undermine Ukraine's resilience. The good news is that Ukraine was prepared for cyberattacks. In regard to the problems of critical infrastructure. In this context, global interconnected infrastructure is being used to conduct attacks. Concerning the capacity of the private sector, the private sector has been learning for years how to protect itself and that the protection of systems is never perfect. However, there are greater capacities now in the private sector and in Ukraine to avoid cyber destruction. We must not forget that it was foreseen that the war against Ukraine would be short and therefore Russia might not aim to destroy the internet infrastructure. The experts did not see such massive destruction as might have been expected. In terms of the infrastructure, it has been reported that when there was the destruction caused in some towns, there was a rapid distribution of sim cards to the population to re-route the network to control the ways how the population accesses information. It is not a question of destroying the infrastructure as much as adapting it.

Mr. Duguin further spoke about the importance of investments in cyber resilience, including in SMEs, administrations and the public sector which are under-protected because they are under-resourced. If these parts of infrastructure cannot be protected in peacetime, it is impossible to protect them in wartime. There is a global underinvestment across the board. The legal frameworks proposed by the EU must be matched by the allocation of necessary resources to meaningfully improve cyber resilience. In regard to the earlier question about the Wagner Group, the Institute looked into the cybercriminal groups taking positions at the beginning of the war. After the mutiny in Russia, there was silence in cyber communities. Concerning the links between the Wagner Group and criminal groups, the Institute does not have data at this stage. To conclude with a response to the question on synthetic content on online platforms, some studies suggest that in 2-3 years, more than 80% of online content will be fake. Organizations currently do not have the detection capabilities to evaluate all this content. DSA is an important step forward, but the EU must bring it to the operational level.

Pavlina Pavlova, Public Policy Advisor, CyberPeace Institute, underscored that the question of scope and frequency of cyberattacks is among the key questions regarding the use of cyber in the war against Ukraine. There are several explanations for this. To begin with, Ukraine was prepared for cyberattacks. The country was for many years a trial ground for Russia to try different kinds of cyberattacks and operations long before the invasion. The effect of any attack relies on the moment of surprise, and Ukraine was not surprised by Russian cyberattacks. The country was preparing over the years, in cooperation with the EU, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and the private sector represented by both international and national companies. This is also a reason why this recommendation for further cooperation across sectors is part of the working paper because the Institute saw how important it was to invite many entities to collaborate. It is also important to include many entities in this collaboration. For example, NGOs are often targeted by cyberattacks, together with think tanks, and research organizations – because if everyone can be a perpetrator in cyberspace, everyone can be a target as well. At the same time, these organizations deliver important threat intelligence, capacity building, and knowledge. In terms of the novelty of cyberattacks, the Institute did not see new attacks, but we recorded attacks that were deployed before such as disruptive attacks and hack and leak operations. These attacks have been present for a long time now they are more concentrated. The number of cyberattacks increased massively with the invasion of Ukraine. The cyber dimension is very much present in this war, but kinetic weapons are easier to be deployed and cause massive destruction. Cyberattacks have more strategic value when there is not an open war. What can be seen as of strategic value of the use of cyber as part of this war, is the coordination between kinetic and cyberattacks and operations. The details can be found in the report and on the publicly available online platform created by the CyberPeace Institute. For all, the Viasat case can be mentioned as a well-known cyberattack. It was a sophisticated wiper malware attack that was deployed right at the beginning of the invasion when tanks were rolling into Ukraine. The malware aimed to affect the command systems of Ukraine. Certain levels of coordination were also observed later, in cases of public administration being hit by cyberattacks shortly before cities were targeted by missiles. The CyberPeace Institute also recorded many attacks on the energy sector, especially during the winter. Those parts of critical sectors are being paralyzed or attempted to be paralyzed by cyberattacks and hit by traditional weapons. This coordination then delivers the strategic impact for the course of the war. Additionally, sophisticated attacks are difficult to design, deploy, and predict in regard to their impact. This is part of the equation of why there has not been a large number of such attacks deployed over the course of the war. A high frequency of sophisticated attacks was observed at the beginning of the war as it could have been assumed that the war would be short. Also, because of the early Viasat attack and its spillover effect, there could be the calculation that if these kinds of destructive attacks are deployed they could potentially meet a threshold for an answer from non-belligerent countries. While lots of cyberattacks have happened against countries allied to the two belligerent countries, none of which seem to have been taken as meeting a threshold of a response. Continued analysis will need to be made of cyber incidents as information becomes available including to assess if and which attacks meet a threshold for accountability including prosecutions before, for instance, the International Criminal Court. Finally, while there has not been a lot of innovation in the types of attacks observed as part of this war, it also must be taken into consideration that with new technology such as generative AI and large language models, both cyber defence and cyber offence can be bolstered. It is therefore key not to underestimate the future impact of cyberattacks in warfare. For example, Ukraine has been using AI for detecting vulnerabilities in their systems and then accordingly supporting these systems, and advanced technologies will play a gradually more important role as they evolve.

5 Biographies of speakers

Stéphane Duguin, Chief Executive Officer, CyberPeace Institute, Geneva

Stéphane Duguin is the CEO of the CyberPeace Institute. He has spent two decades analysing how technology is weaponized against vulnerable communities. In particular, he investigates multiple instances of the use of disruptive technologies, such as AI, in the context of counter terrorism, cybercrime, cyber operations, hybrid threats, and the online use of disinformation techniques, notably at Europol. He leads the CyberPeace Institute with the aim of holding malicious actors to account for the harms they cause. His mission is to coordinate a collective response to decrease the frequency, impact, and scale of cyberattacks by criminal groups and state actors. Stéphane Duguin sits on the Board of the Datasphere Initiative and is a member of the Advisory Board of the Open Quantum Institute, the Global Forum on Cybercrime Expertise (GFCE), the Tech4Trust initiative, the Fighting Terrorist Content Online (FRISCO) and the Global Cyber Alliance (GCA). Stéphane Duguin also served in EUROPOL as senior manager in the European Cybercrime Centre (EC3), the European Internet Referral Unit (EU IRU), and the EUROPOL Innovation Lab.

Pavlina Pavlova, Public Policy Advisor, CyberPeace Institute, Geneva

Pavlina Pavlova is Public Policy Advisor at the CyberPeace Institute, where she works on advancing international law and norms in cyberspace. Prior to this role, Pavlina was an official at the Organization for Security and Co-operation in Europe (OSCE), being appointed Liaison Officer of the OSCE Chairmanship. As an international expert, she also coordinated OSCE capacity-building programmes in Ukraine aimed at strengthening the human dimension of security. Pavlina has been publishing and speaking on the nexus between technology, human rights, and security. Her research centres around cyber threats impacting vulnerable and targeted groups and the interlink between online and offline security. She authored research papers on information control technology, platform governance, and content moderation presented at the Yale MacMillan Center, the Carr Center for Human Rights Policy of the Harvard Kennedy School, and the Stanford Internet Observatory, among other fora.

6 Photos from the workshop

All photos: © European Union 2023 – EP/Alexis Haulot

PE 702.594
EP/EXPO/SEDE/FWC/2019-01/LOT4/1/C/20

Print ISBN 978-92-848-0885-4 | doi: 10.2861/019965 | QA-07-23-249-EN-C
PDF ISBN 978-92-848-0884-7 | doi: 10.2861/800788 | QA-07-23-249-EN-N